

INTERNAL AUDITOR'S REPORT
Huntington Union Free School District
For the 2013-2014 Fiscal Year



437 Madison Avenue, 29th Floor
New York, NY 10022 • 212.962.4470

165 Orinoco Drive, Brightwaters, NY 11718
631.665.7040 • Fax: 631.665.7014

15 South Bayles Avenue, Port Washington, NY 11050
516.883.5510 • Fax: 516.767.7438

A PROFESSIONAL CORPORATION OF CERTIFIED PUBLIC ACCOUNTANTS

www.sheehancpa.com

May 30, 2014

Board of Education and Audit Committee
Huntington Union Free School District
Administrative Offices
50 Tower Street
Huntington Station, New York 11746

To the Members of the Board of Education and Audit Committee:

In accordance with the terms of our engagement with the Huntington Union Free School District we have performed the District's annual risk assessment update as required by Chapter 263 of the Laws of New York of 2005 for the 2013-2014 school year.

Chapter 263 of the Laws of New York of 2005 requires that school districts establish an internal audit function to perform a risk assessment of district operations including, but not limited to, a review of financial policies and procedures and the testing and evaluation of district internal controls.

Internal controls are procedures put in place by management to help achieve the stated mission and objectives of an organization. The design and implementation of internal controls is the responsibility of management. These control procedures help promote efficiency in operations, reduce risk of loss and ensure reliability of financial data. In addition, internal controls are designed to provide reasonable, but not absolute, assurance regarding the achievement of the entity's objective to promote compliance with established policy, laws and regulations. The concept of reasonable assurance recognizes that the cost of internal control should not exceed the benefits derived. There are inherent limitations that should be recognized in considering the potential effectiveness of any internal control system such as errors, mistakes of judgment, carelessness, collusion or other factors.

Annual Risk Assessment

Risk assessment is the entity's identification and analysis of relevant risk to the achievement of its objectives, forming a basis for determining how the risks should be managed. It should identify risk and analyze the likelihood of occurrence and impact. This process allows the Board of Education to determine how much risk it is willing to accept and to set priorities accordingly. The assessment should focus on what can go wrong that would prevent the achievement of the objectives, the likelihood and consequences of something going wrong, and what actions can be taken to minimize the potential of occurrence.

In assessing risk, we consider both inherent risks: the risk associated with a system based upon the nature of the transactions processed by that system (i.e. quantity, complexity, value, etc.) and control risk: the risk that the system of internal control is not adequately designed to prevent or detect errors or irregularities.

Risk assessment is an ongoing internal audit function. This process includes a review of policies, procedures and controls that the District has in place to prevent errors, detect fraud, safeguard District assets and ensure that financial reporting is accurate. Interviews and checklists are utilized to confirm our understanding of the control process and assess changes in risk, with an emphasis on increased risks related to changes in key personnel, changes in policies, laws and regulations and new policies, laws and regulations. The scope of our risk assessment engagement did not include testing the operating effectiveness of such controls. Risk assessments of key operational and financial areas are documented in a matrix to facilitate monitoring of risks on an annual basis.

Our procedures were not designed to express an opinion on the internal controls of the District, and we do not express such an opinion. Because of inherent limitations of any internal control, errors or fraud may occur and not be detected by internal controls. Also, projections of an evaluation of internal controls to future periods are subject to the risk that procedures may become inadequate because of changes in conditions.

The key operational and financial areas include the following general categories:

- Governance and Planning
- Accounting and Reporting
- Revenue and Cash Management
- Grants
- Special Education
- Payroll
- Employee and Retiree Benefits
- Human Resources
- Purchasing and Expenditures
- Facilities
- Fixed Assets
- Safety and Security
- Food Service
- Extraclassroom Activity Fund
- Student Related Data
- Information Systems

The risk assessment matrix was reviewed by the District in November 2013. Upon review of the risk assessment matrix, the audit committee directed us to perform detailed testing/evaluation procedures in one or more key areas.

Detailed Testing/Evaluation Procedures

As a result of the risk assessment process, with the assistance of the District's audit committee and management, tests have been designed to evaluate the effectiveness of existing internal controls and their implementation in the following area(s):

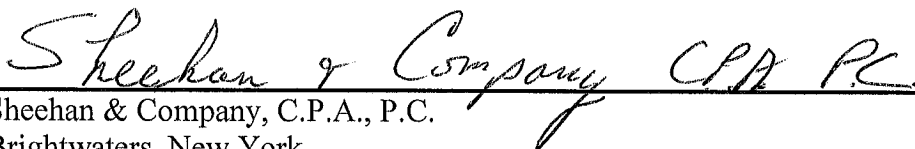
- Privacy and Protection of Data – Employee Data (pages 6 - 13)
- Privacy and Protection of Data – Student Data (pages 15 - 22)
- Privacy and Protection of Data – Information Technology (IT) Environment (pages 23 - 41)
- Privacy and Protection of Data – Business Office and Administration (pages 42 - 46)

We have performed the testing and evaluation for the operational/financial area(s) listed above. The results of this testing and evaluation, as well as our findings, recommendations and management's response are reported in the following section. As part of the ongoing internal audit function, we will continue to assess and monitor the implementation of any corrective actions deemed necessary.

This report is intended solely for the use and information of the Board of Education, Audit Committee and management of the Huntington Union Free School District and is not intended to be and should not be used by anyone other than these specified parties.

We appreciate the opportunity to serve you as internal auditors and thank the District's management and staff for their assistance and cooperation.

Very truly yours,



Sheehan & Company, C.P.A., P.C.
Brightwaters, New York
May 30, 2014

Introduction - Privacy and Protection of Data

The focus of this internal audit is to determine whether the District has implemented policies and procedures to regulate the processing and protection of personal data and that processing is carried out in accordance with such policies and procedures.

The importance of the protection of data, both employee and student, should not be underestimated, as security breaches can come at a high price. In the Internet Age, one computer that is not properly protected, or one hard drive that is not adequately erased, can provide thieves with access to thousands of personal records which they can use to apply for credit cards, spend money that isn't their own and wreak havoc on the lives of those whose data was compromised.

When examining the internal controls protecting personal and sensitive data, it is important to understand the data life cycle, because different stages may require different types of controls:

- **Data at rest** refers to data storage, whether in file cabinets or on a server.
- **Data in motion** refers to data transfer, which is primarily used when data is being exchanged electronically, but also when physical files are moved.
- **Data presentation**, also known as data in use, refers to data that is being used or accessed, including such outcomes as being displayed on a monitor.
- **Data destruction** refers to steps organizations take when they no longer need access to certain data. Controls over shredding paper files, overwriting hard drives, and other tasks come into play.

Data maintained by school districts, both paper and electronic, will include social security numbers for employees and students, financial account information, medical records, employee and student evaluations, and disciplinary records, all of which is subject to misuse if not adequately protected. In the case of electronic records the risks of data breach are much greater with data being so easily copied and transferred to mobile computing devices (MCD's) such as laptop computers, iPads, smart phones, and other electronic devices. The electronic environment increases the risk of unauthorized access, disclosure, modification and deletion of an employee's or student's personal, private, and sensitive information (PPSI). Districts can reduce such risks by developing and enforcing policies and procedures to assure that PPSI is secured through proper controls.

Some key issues that the District should consider as it develops, updates and implements its data protection policies and procedures include:

- **Paper documentation** - With all the attention given to electronic devices, it is important not to overlook the security risks associated with traditional physical records. Something as simple as having a "clean desk" policy, requiring employees to put all documents away before leaving the office/classroom, can help reduce the chance of data breaches.

- **Mobile devices** - As smartphones, tablets, and other portable devices proliferate, so do the risks of data breaches. The District needs to continually address emerging technologies in its data protection policies.
- **Social media** - Like mobile devices, social media is likely present in the workplace. Someone may post an inappropriate comment or disclose personal/sensitive information on the Internet about a student or colleague. The District needs to consider how its employees' use of social media could affect data privacy.
- **Third parties** - Sharing sensitive information with third parties expands the circle of risk beyond the District's walls. Managing this risk is not easy and requires vigilance by all parties involved.
- **Breach notification** - Alerting parents, students, employees and regulatory authorities to data breaches is another challenge for school districts, which must balance researching what happened with the timeliness of their notification to impacted individuals. The District needs to have clearly defined procedures in place and rehearse its response so that everyone knows what to do when a breach occurs.

The importance of data protection and related risks is now being recognized by the Office of the New York State Comptroller. Over the last four years the Comptroller's auditors have been focusing on data security policies in school districts. From January 1, 2010 through May 4, 2012 the Comptroller's office conducted a comprehensive review of the policies and procedures to protect PPSI in twelve school districts throughout New York State and released its report in December 2012. The results were alarming. The Comptroller's auditors found that the majority of the districts did not have adequate security policies and procedures in place, increasing the risk that PPSI could be accessed and misused by unauthorized persons.

Privacy and Protection of Data - Employee Data

Overview

In the normal course of its operations, the District will collect and use personal data belonging to job applicants, employees, and retirees for many purposes including certifications, evaluations, compensation, and benefits.

The purpose of a data protection policy is to set out the conditions under which the District will process personal data and ensure that everyone in the District is aware of their individual responsibilities and the District's expectations regarding privacy.

By having an employee data protection policy, the District can reduce the risk of claims for failing to comply with data privacy laws and give itself greater flexibility to monitor an employee's use of email, the internet and other devices where necessary.

Personal data is information that relates to a living person who can be identified from that data. This includes an individual's personal details and personnel file and any expression of opinion about or understanding of facts concerning the individual. The protection of employee data by employers is required throughout the employment relationship.

A data protection policy should be tailored to the District's operations to take account of the structure of its organization, resources and particular personal data which it may process. A policy must then be communicated to staff and monitored in practice. The policy should also indicate the measures to be taken by the District to ensure that there are appropriate security measures in place to safeguard employee data and address how this will be protected when the District transfers employee data outside of its direct control (as with third parties, or software that processes and stores data "in the cloud").

For an employer, the consequences of not protecting personal data have been underscored by court rulings and state and federal laws that seek to hold custodians of sensitive information responsible for diligently protecting the data they obtain, and subject to penalties if they don't. Safeguarding and properly disposing of personal information in all forms has become a business necessity for school districts for a variety of reasons, including potential legal liability, reputation, and employee confidence.

When considering the life cycle of employee records, employers should focus, in broad terms, on data input, storage and disposal. Although there are no easy answers about the best ways to collect, manage and dispose of such sensitive information, employers can, and should, take sufficient steps to ensure the security of employee data.

A number of breaches of employee and student data have occurred and been reported in the news over the last year or so. As a result, now, more than ever, it is important that all school districts consider putting in place a data protection policy if none exists, or review existing policies to ensure these remain relevant and effective.

Employee Data

Objective

Taking into consideration the functional components of both paper and electronic employee data, develop a knowledge base which represents the District's understanding and implementation of the data protection policies and procedures as is applicable to this area of records.

Procedures

Questionnaires were developed that addressed key areas of employee data maintained in both paper and electronic form. These questionnaires were sent to the individuals responsible for the following areas:

- Compensated absences
- Disciplinary
- Employee benefits
- Evaluations
- Payroll records
- Personnel records

Responses were compiled. Some respondents provided copies of documents to support/illustrate their replies. Follow-ups were conducted to clarify any responses received that were unclear or for which we determined additional information was necessary.

Findings

Section One - Paper Records

The following are the questions posed as pertains to *paper records* containing employee data. A synopsis of our findings and recommendations are presented after each question.

- *Are there written policies and procedures relating to access rights, security, privacy rights, compliance with laws, retention period, method of disposal, etc.? Please provide a copy.*

The majority of respondents believe that policies exist, but don't have copies to refer to. One respondent referred to *New York State Schedule ED-1 - Records, Retention and Disposition*, but no one could provide us with any actual District policies.

The District does, in fact have a number of policies that address many of these issues related to data/records.

Employee Data - Paper Records

Recommendation:

The District has adopted the New York State Schedule ED-1 as pertains to record retention in Policy # 5670. Policies related to the areas of access rights, security, privacy rights, and compliance with laws have been adopted by the District in the past. However, it is apparent that many of the District's employees are not aware of the policies. We suggest that these policies be communicated to personnel handling employee data and copies made available for their reference.

- *A common practice is that persons granted access to personally identifiable data be required to sign an "oath of non-disclosure". Does the District require employees to sign an "oath of non-disclosure", or a similar acknowledgement of an employee's duty to keep personal information confidential?*

None of the respondents were aware of an "oath". One respondent provided a packet of policies and regulations that is provided to new hires which includes a clause about confidential information (policy 6110 (b) Code of Ethics). The packet requires a signature indicating "review and comply with the Policies and Regulations." (See **Appendix A**)

Recommendation:

We noted that the new hire packet addresses Confidential Information in the Code of Ethics section and that the topic consists of a single sentence. It was also noted that the Code of Ethics policy (#6110) was adopted in the year 2006. While at that time, a single sentence may have been sufficient, in the current environment of data risks and breaches it would be prudent to expand the language addressing the topic - perhaps creating a separate and specific policy.

The "oath of non-disclosure" is a recommendation of the National Center for Education Statistics, U.S. Department of Education which requires that its employees granted access to personally identifiable data be required to sign the oath. The document itself should list all types of information that must be kept confidential and forbid staff from discussing security aspects of the data system, whether a locked filing cabinet or a computer, with unauthorized individuals. Specific penalties required by law or regulations should be included in this oath. They acknowledge that while this may seem extreme, it can help to ensure that staff knows exactly what the requirements and their responsibilities are.

- *Where are current records physically kept? / How are records secured?*

The general response was that records are kept in locked file cabinets or a locked office.

Employee Data - Paper Records

Recommendation:

It is important that personal/sensitive records are maintained in locked file cabinets. It is suggested that this be addressed in a formal, written policy. Verifying that the cabinets have locks, that the locks work and that the procedure is to physically lock the cabinet (and not leave the key hanging from the lock) when the office is left unattended would be a valuable exercise.

- *What is the District's retention policy for the type of record for which you are responsible? / After what period of time would a current record be transferred to archives? / How are records disposed of/destroyed? /Who is accountable for its disposal/destruction?*

Although most respondents were unaware of the District's retention policy, the District Policy # 5670 "Records Management" sets forth the District's retention policy (based on New York State Schedule ED-1).

Recommendation:

It appears that current practices are based upon what "has always been done" as opposed to what has been established and adopted as District policy. If the individuals in the specified areas of inquiry are responsible for record retention and archiving, they should be made aware of/provided with the District's policy as applies to this area. Copies of New York State Schedule ED-1 should be distributed to all employees responsible for records management.

- *How are rights to data access established? / Are access rights updated periodically (for example, for employee terminations, retirements, new employees, etc.)? / Is a documented request required to access the records? / Is a historical log maintained indicating who has accessed the record?*

Most respondents were uncertain how access rights are established, but recognize that they are granted to those that need the data to perform their duties. All acknowledged that access rights are updated periodically and stated that documented requests were neither required for payroll and human resources employees nor for the Assistant Superintendent's office. Historical logs were maintained only by the Personnel and Evaluations areas.

Recommendation:

We recommend that the District develop and adopt formal, written policies that address the issues of establishing data access rights, when and how access rights should be granted or removed, and when (and for what data) document requests and logs should be required.

Employee Data - Paper Records

- *Do you receive requests from third parties (non-employees of the District) seeking records? / Are there procedural guidelines to deal with requests for personal data from third parties? Please provide a copy. / Do you document all requests received and responded to?*

None of the respondents are aware of a formal policy/procedure in this area. Some indicated that there were no procedural guidelines; others referred to an employee consent form and court orders. All respondents agree that they document third party requests by retaining applicable copies in the employees' files.

Recommendation:

Although it appears that information would not be released to a third party without careful consideration as to the legitimacy of the request, it is recommended that a policy/procedure be established that clearly indicates the documentation required in order to release information to a third party. We noted a packet of student "release of information authorization forms" included as a component of the District's policies and procedures; we did not, however see a form specifically applicable to employees and an authorization to release their information. A standardized employee consent form should be used in all instances of such requests (with the exception of a court order).

District Policy # 6420 and related regulations provide the procedures for obtaining consent for the release of records to third parties. As the District's employees are not aware of the policies, the policy and consent form should be provided to all employees handling employee data.

- *May a person with appropriate rights remove the record from the file storage area? / May a person with appropriate rights make a copy of the record? / Is there a mechanism to detect alterations (authorized or unauthorized) to a particular record?*

All responses indicated that the record could be removed from the file storage area and copied by a person with appropriate access rights. All respondents said there was no mechanism in place to detect alterations.

Recommendation:

In the course of daily business it is reasonable for people within the payroll and human resources areas to remove and/or copy files as needed. We acknowledge that personnel realize the confidential nature of these files, however, removal and copying files can introduce risks:

- How are the removed files secured while being "borrowed"?
- Is there a requirement to return the files before the end of the day?

Employee Data - Paper Records

- Is there a procedure to ascertain that all removed files are returned?
- How are the copied files secured?
- What is done with copied files when the copies are no longer needed?
- Assuming the copies are destroyed, are they shredded (preferably cross-cut, diamond-cut, or confetti cut)?

Policies and procedures always need to take into account the District's operations, structure and resources, but should be developed and/or updated with the above concerns in mind. Inappropriate access of removed or copied files can be accidental or intentional. Securing against inappropriate access needs to be taken into consideration. Restricting physical access to storage areas, recording sign in and sign out of files and maintaining records handling training are some policies/procedures that can be considered.

Unauthorized data alteration is an important concern in the area of data security. Anyone who has access to the paper record can remove pages, add entries or otherwise tamper with the authorized data. Detection of such "tampering" is difficult to implement, but it is an administrator's responsibility to inspect a record after it has been accessed by another employee (in accordance with Policy # 6420-P).

- *Are the records for which you are responsible subject to any compliance with laws, regulations or other regulatory requirements? / Health Insurance Portability and Accountability Act (HIPPA)? / NYS Department of Education? / Other? / What controls are in place to assure compliance with laws, regulations or other regulatory requirements?*

HIPPA was noted in a few responses. Another noted Sheriff, County Offices, IRS and NYS Tax Department. Most did not know if controls were in place to assure compliance with laws, regulations or other regulatory requirements. One respondent noted that when requests come in they are accompanied by instructions and compliance documentation.

Recommendation:

Policies and procedures should be developed and adopted in a manner that ensures compliance with laws and regulatory requirements. District personnel may not be aware of all legal/regulatory compliance issues and may be in need of guidance to assure that all requirements are complied with.

Section Two - Electronic Records

Many of the same questions detailed above, as applicable to paper records, were asked as they pertain to electronic records and the same responses were received. In order to avoid redundancy, the following are the unique questions posed as pertains to electronic records

Employee Data - Electronic Records

containing employee data or those for which different responses were received as compared to responses pertaining to paper records. A synopsis of our findings and our recommendations are presented after each question.

- *Is the information accurate, complete and up-to-date? / Is there a system in place to assure the information is accurate, complete and up-to-date?*

Generally, respondents indicated that the information was in fact accurate, complete and up-to-date. Of the three respondents that indicated that there is a system in place to assure the information is accurate, complete and up-to-date, two stated Microsoft Access is the system that provides this assurance. Several respondents indicated they did not know.

Needless to say, information that is not accurate, complete or up-to-date is not useful, and, in some cases, may have significant negative consequences. There are three questions related to this topic which are essential to address in order to have some level of assurance that the data is accurate and complete:

- Do we check our data for accuracy?
- Do we know how much of our data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?
- Do we take steps to ensure our databases are kept up-to-date?

From the responses received, it is difficult to ascertain whether such procedures are in place. Microsoft Access, in and of itself, does not provide such assurance. It is difficult to implement procedures to ensure accuracy and completeness in every situation. However, it is an implicit expectation that every District employee will diligently maintain the records for which they are responsible.

- *Where is the data physically stored? By a third party (i.e. BOCES)?*

Responses included NYSHIP (New York State Health Insurance Program), MetLife, BOCES, Finance Manager and other third parties.

- *Is a password required to access the records? / Is there a policy to change passwords periodically?*

Each respondent acknowledged that passwords are required, but on the topic of changing passwords periodically, only Finance Manager and IEP Direct were identified as requiring that passwords be changed periodically. Respondents using other software applications indicated the passwords were not changed periodically.

Employee Data - Electronic Records

Recommendation:

Please refer to the IT section of this report for specific information pertaining to passwords, but in general, a strong computer password, which is changed periodically, is an important means to prevent unauthorized access to data.

- *Is a historical log maintained indicating who has accessed the record?*

For Finance Manager and the New York Benefits Eligibility and Accounting System, respondents answered "yes". For all other software applications, the indication was that historical logs are not maintained.

Recommendation:

Historical access logs provide the ability to monitor access to and changes to data. Using this monitoring tool will facilitate the process of detecting, and perhaps preventing, unusual/unauthorized activity.

Please refer to the IT section of this report for more information.

- *May a person with appropriate rights to access the data, transfer the data to another device such as a flash drive, laptop, or iPad?*

Some respondents said yes, while others said no. No one was aware of any District policy.

Recommendation:

As mentioned in the IT section of this report, the District should enhance, update and communicate its policies related to data access and protections in the IT environment. The risks to data security are greatly increased when data is transferred to mobile devices. Once data is transferred from the District's network it is difficult to control access to the data, or prevent the device from being lost, along with the personal/sensitive data.

A policy regarding the use of mobile data devices should include the following:

- Only flash drives, or other mobile devices, secured by the IT department should be used. These should all be tracked to ensure the District knows at any given time who is using which drive and for what purpose.
- All data that is transferred to a flash drive should be encrypted. Ensure that the encryption process is automatic to avoid this being forgotten and the copied data become vulnerable to unauthorized access.

Privacy and Protection of Data - Student Data

Overview

In general, the same basic concepts regarding policies and procedures for protecting the data of employees would also apply to student data. However, the protection of student data rises to an even higher level due to protections provided by federal and state laws.

Students and their parents entrust schools with their personal information with the expectation that this information will be used by the schools to serve the needs of the students effectively and efficiently. School districts maintain and use personal information for a variety of educational purposes while students are in school. To protect the privacy of the students and their families, school employees and officials are legally and ethically responsible for safeguarding student information.

To protect the privacy of families whose children are in school, states and the federal government have established strong legal statutes to keep private the information in education records that schools maintain on students. These laws frame data collection procedures, restrict information disclosure, and safeguard the quality of the information that school systems routinely collect and maintain. All education records about students, whether handwritten or computerized, are protected by the same privacy regulations.

In addition to the everyday use of student information by teachers and administrators, education records are a source of basic data used for administrative purposes and policymaking. Administrative use of computerized records means that education records are used increasingly farther from their point of origin. As a result, it has become more complicated, but no less essential, for school officials to be vigilant about protecting the confidentiality of records. Those who work with education records have legal and ethical obligations to observe rigorous procedures for protecting the privacy of the original information and the individuals whose records are involved.

Family Educational Rights and Privacy Act (FERPA)

Student education records are official and confidential documents protected by one of the nation's strongest privacy protection laws, the Family Educational Rights and Privacy Act (FERPA). FERPA defines education records as all records that schools or education agencies maintain about students.

FERPA gives parents (as well as students in postsecondary schools) the right to review and confirm the accuracy of education records. This and other United States "privacy" laws ensure that information about citizens collected by schools and government agencies can be released only for specific and legally defined purposes.

Student Data

FERPA applies to public schools and state or local education agencies that receive Federal education funds, and it protects both paper and computerized records.

FERPA requires schools and local education agencies to annually notify parents of their rights under FERPA. The annual notice pertaining to FERPA rights must explain that parents may inspect and review records and, if they believe the records to be inaccurate, they may seek to amend them. Parents also have the right to consent to disclosures of personally identifiable information in the record, except under authorized circumstances.

When students reach the age of 18, or when they become students at postsecondary education institutions, they become "eligible students" and rights under FERPA transfer to them. However, parents retain access to student records of children who are their dependents for tax purposes.

Education records, as defined by FERPA, include a range of information about a student that is maintained in schools in any recorded way, such as handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche. Examples are:

- Date and place of birth, parent(s) and/or guardian addresses, and where parents can be contacted in emergencies;
- Grades, test scores, courses taken, academic specializations and activities, and official letters regarding a student's status in school;
- Special education records;
- Disciplinary records;
- Medical and health records that the school creates or collects and maintains;
- Documentation of attendance, schools attended, courses taken, awards conferred and degrees earned;
- Personal information such as a student's identification code, social security number, picture, or other information that would make it easy to identify or locate a student.

Personal notes made by teachers and other school officials that are not shared with others are not considered education records. Additionally, law enforcement records created and maintained by a school or district's law enforcement unit are not education records.

Part of the education record, known as *directory information*, includes personal information about a student that can be made public according to a school system's student records policy. Directory information may include a student's name, address, and telephone number, and other information typically found in school yearbooks or athletic programs. Other examples are names

Student Data

and pictures of participants in various extracurricular activities or recipients of awards, pictures of students, and height and weight of athletes.

Each year schools must give parents public notice of the types of information designated as directory information. By a specified time after parents are notified of their review rights, parents may ask to remove all or part of the information on their child that they do not wish to be available to the public without their consent.

Local education agencies and schools may release information from students' education records with the prior written consent of parents, under limited conditions specified by law, or as stated in local agencies' student records policies. The same rules restricting disclosures apply to records maintained by third parties acting on behalf of schools, such as state and local education agencies, intermediate administrative units, researchers, psychologists, or medical practitioners who work for or are under contract to schools.

If an education agency or a school district has a policy of disclosing records, it must specify the criteria for determining school officials within an agency, including teachers, who have a legitimate educational interest. Generally, school officials have legitimate educational interest if they need to review an education record to fulfill their professional responsibilities.

Information from students' records may be released to state and local education officials to conduct audits or to review records in compliance with Federal laws. Schools may also disclose information from education records without the consent of parents in response to subpoenas or court orders. A school official must make a reasonable effort to notify the parent before complying with the subpoena unless the subpoena is issued to enforce a law and specifies not to notify the parent.

Schools that participate in a federally assisted school nutrition program have personal information about students' eligibility for free and reduced-price school meals or free milk. These programs have regulations that are more restrictive than FERPA's regarding the disclosure and use of this information.

Because of the many rights and privacy protections granted by FERPA, it is important that the District has effective policies and procedures in place to ensure compliance with its many provisions. It is also important that all District employees are kept aware of FERPA's provisions.

Student Data

Objective

Taking into consideration the functional components of both paper and electronic employee data, develop a knowledge base which represents the District's understanding and implementation of the data protection policies and procedures as is applicable to this area of records.

Procedures

Questionnaires were developed that addressed key areas of student data maintained in both paper and electronic form. These questionnaires were sent to the individuals responsible for the following areas in each of the District's schools:

- Academic
- Attendance
- Disciplinary
- Health
- School Lunch Program
- Special Education

Responses were compiled. Some respondents provided copies of documents to support/illustrate their replies. Follow-ups were conducted to clarify any responses received that were unclear or for which we determined additional information was necessary.

Findings

Section One - Paper Records

Many of the same questions applicable to student paper records were asked in previous sections of this report and the same responses received. In order to avoid redundancy, the following are the questions posed for which it was deemed informative to present responses. If the question was addressed in a previous section, our recommendation is not repeated here - reference is provided as to where it has already been cited in our report.

- *Are there written policies and procedures relating to access rights, security, privacy rights, compliance with laws, retention period, method of disposal, etc.? Please provide a copy.*

The majority of respondents believe that policies exist, but don't have copies to refer to. One respondent provided a document entitled "Huntington Union Free School District Food & Nutrition Department Retention of Records" (See **Appendix B**). This document appears to have been extracted from New York State Schedule ED-1.

Student Data - Paper Records

Recommendation:

The District adopted Policy # 7240 "Student Records" in 2003. This policy addresses privacy rights and compliance with laws. District Policy # 5670 "Records Management", adopted in 2001, incorporates the retention policies of New York State's Records Retention and Disposition Schedule ED-1. However, we did not find any evidence of District policies that address access rights to records, security of records, or disposal of records. We suggest that the District develop and adopt policies to address these issues.

As our findings indicated that District employees do not have copies of District policies, nor do they know where to find them, we suggest that the District take steps to ensure that its employees are aware of existing policies. If an employee is not aware of a policy, there is great risk that an employee's actions are not in compliance with the policy.

- *A common practice is that persons granted access to personally identifiable data be required to sign an "oath of non-disclosure". Does the District require employees to sign an "oath of non-disclosure", or a similar acknowledgement of an employee's duty to keep personal information confidential?*

The general answer from this group of respondents was "no". Several of the respondents referred to the confidentiality agreement included in the new hire packet (see **Appendix A**). The Special Education Department has the equivalent of an oath - in IEP Direct, all parties sign this form. Two of the school nurses responded that they have their own oath of confidentiality which is taken upon passing the Board exam and obtaining their license.

Recommendation:

Please refer to the recommendation in Employee Data - Section One - Paper Data.

- *What is the District's retention policy for the type of record for which you are responsible? Please provide a copy. / After what period of time would a current record be transferred to archives? / How are records disposed of/destroyed? / Who is accountable for its disposal /destruction?*

The majority of respondents were unaware of a retention policy or a records disposal/destruction policy. Although there was no consistent response as to after what period of time would a current record be transferred to archives, a couple of respondents did provide similar responses. They indicated that students' folders follow them to the next school within the District as they progress through to grade level 12. One respondent indicated that the method of disposal was that records were thrown out; the secretary in charge of the section marks boxes for disposal and custodian throws them out.

Student Data - Paper Records

Recommendation:

It appears that current practices are based upon what "has always been done" as opposed to what has been established and adopted as District policy, as most employees are not aware of District policy. If the individuals in the specified areas of inquiry are responsible for record retention and archiving, they should be made aware of/provided with the District's policy as applies to this area. District Policy # 5670 "Records Management", adopted in 2001, incorporates the retention policies of New York State's Records Retention and Disposition Schedule ED-1. We suggest that the District take steps to ensure that its employees are aware of the existing retention policy.

We did not find any evidence of District policies that address how records are to be disposed of, or who is responsible for the disposal of records. We suggest that the District develop and adopt policies to address these issues.

- *Are there procedural guidelines to deal with requests for personal data from third parties?*

Most of the respondents were not aware of a formal District policy or procedure. One referred to a District "Request for Records" form. Others provided copies of forms they use for this purpose. One provided the forms that were included as a component of the District's Policies and Procedures (see **Appendix C**).

District Policy # 7240 "Student Records", adopted in 2003, and its related regulations, provides policy regarding disclosure of student records to District personnel, as well as professionals with whom the District has contracted, such as an attorney, auditor, medical consultant, or therapist.

Recommendation:

Although it appears that information would not be released to a third party without careful consideration as to the legitimacy of the request, it is recommended that a policy/procedure be established that clearly indicates the documentation required in order to release information to a third party. We noted a packet of student "release of information authorization forms" included as a component of the District's policies and procedures. These forms should be provided to, and used by, all persons in areas handling employee data.

It is important to note that FERPA restricts the release of student data without prior consent. Without consent of the parent of an eligible student, education records can be disclosed only to school officials designated as having a "legitimate educational interest". The law leaves to the District the authority to define the criteria for determining the legitimacy of an educational interest, which generally includes situations where officials

need to review education records to fulfill their professional responsibilities. This includes access to records by teachers, counselors, and administrators who routinely work

Student Data - Paper Records

with students. The following lists some example situations in which legitimate educational interest prevails:

- To perform education- or discipline-related tasks in connection with a student
- To provide services to a student or a student's family such as emergency health care, counseling, or school or job placement
- To perform administrative or other educational responsibilities prescribed by the school

If an educational agency or institution has a policy of disclosing education records to officials considered to have a legitimate educational interest, it must also give annual notification that explains the criteria for determining who constitutes a school official and who constitutes legitimate educational interest. District Policy # 7240 "Student Records" requires that the District publish a notification at the beginning of each school year. Disclosure of information to an individual or agency outside the school, school district, or state education agency - a third party - is not allowed without prior consent of a parent. Under certain circumstances (e.g. government-required audits, evaluations, or court orders), a district can release records without approval of the parent, but it must make clear the criteria for determining which institution or agency representatives may receive such information and under what conditions.

- *Is the information accurate, complete and up-to-date? / Is there a system in place to assure information is accurate, complete and up-to-date?*

Most respondents replied "yes" to the inquiry as to whether information was accurate, complete and up-to-date. Most answered "yes" as to whether there is a system in place to assure information is accurate, complete and up-to-date.

Recommendation:

Information that is not accurate, complete or up-to-date is not useful, and, in some cases, may have significant negative consequences. There are three questions related to this topic which are essential to address in order to have some level of assurance that the data is accurate and complete:

- Do we check our data for accuracy?
- Do we know how much of our data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?
- Do we take steps to ensure our databases are kept up-to-date?

Student Data - Paper Records

From the responses received, it is difficult to ascertain whether such procedures are in place. It is difficult to implement procedures to ensure accuracy and completeness in every situation. However, it is an implicit expectation that every District employee will diligently maintain the records for which they are responsible.

Section Two - Electronic Records

- *A common practice is that persons granted access to personally identifiable data be required to sign an "oath of non-disclosure". Is this a practice in place in the District?*

None of the respondents were aware of an "oath". Reference was made to a packet of policies and regulations that is provided to new hires which includes a clause about confidential information (policy 6110 (b) Code of Ethics). The packet requires a signature indicating "review and comply with the Policies and Regulations." (See Appendix A)

Recommendation:

We noted that the new hire packet addresses Confidential Information in the Code of Ethics section and that the topic consists of a single sentence. It was also noted that the Code of Ethics policy (#6110) was adopted in the year 2006. While at that time, a single sentence may have been sufficient, in the current environment of data risks and breaches it would be prudent to expand the language addressing the topic - perhaps creating a separate and specific policy.

The "oath of non-disclosure" is a recommendation of the National Center for Education Statistics, U.S. Department of Education which requires that its employees granted access to personally identifiable data be required to sign the oath. The document itself should list all types of information that must be kept confidential and forbid staff from discussing security aspects of the data system, whether a locked filing cabinet or a computer, with unauthorized individuals. Specific penalties required by law or regulations should be included in this oath. They acknowledge that while this may seem extreme, it can help to ensure that staff knows exactly what the requirements and their responsibilities are.

- *What controls are in place to assure compliance with laws, regulations or other regulatory requirements?*

Most respondents did not know of any controls. One responded that controls include ongoing training and conferencing; internal self-reviews; peer checks; policies; collaboration with regional associate. Another noted that they follow the rules and regulations of which they are aware.

Student Data - Electronic Records

Recommendation:

Policies and procedures should be developed and adopted in a manner that ensures compliance with laws and regulatory requirements. District personnel may not be aware of all legal/regulatory compliance issues and may be in need of guidance to assure that all requirements are complied with.

Privacy and Protection of Data - Information Technology (IT) Environment

Overview

Data security in an electronic environment is of special concern. The risk of electronic data (both personal and sensitive) being improperly accessed and misused is much greater than with paper records.

In addition to the general data security issues encountered in a paper environment, the electronic data environment introduces many more threats to the security of data. Amongst those threats are the following:

- Viruses and malware
- Hackers and scammers
- Remote access over the internet
- Data storage "in the cloud"
- Web-hosted software applications
- Unattended computers
- Lost laptops, smartphones, iPads and flash drives
- Malicious email attachments
- Use of wi-fi for sensitive activities
- Software vulnerabilities
- Inadequate internet access policies and restrictions
- Disposal of discarded computer devices

District officials are responsible for designing internal controls over information technology (IT) resources that include policies and procedures designed to protect software and data from loss or misuse due to errors, malicious intent or accidents. Such policies and procedures should include an acceptable computer use policy and should address using and monitoring the District's IT system by enabling and periodically reviewing audit trails. District officials should develop written procedures for adding, deleting and changing user access rights within the District's software and ensure that users have only those rights needed to complete their job duties. Further, the District should establish procedures to monitor and control remote access to the District's network by outside vendors and consultants.

Information Technology

An acceptable use policy defines appropriate user behavior and the tools and procedures necessary to protect information systems. Such policies should include, among other things, procedures governing the acceptable use of computers, internet access, email and portable devices and procedures designed to protect the District's resources and confidential information. District officials should distribute acceptable computer use policies to all employees. It is important that such policies include provisions for enforcement and that system users acknowledge that they are aware of and will abide by the policy.

District officials should ensure that there are written procedures in place for granting, changing and terminating access rights to the overall networked computer system and to the specific software applications. These procedures should establish who has the authority to grant or change access (e.g., supervisory approval). Administrator rights allow users to create, delete and modify files, folders or settings, including assigning users' access rights. Generally, a system administrator is designated as the person who has oversight and control of the system and has the ability to add new users and change users' passwords and access rights. With this ability, administrators are able to control and use all aspects of the software. The administrator for the District's finance application should be an individual with no ties to the business office.

Also, to ensure proper segregation of duties and internal controls, it is important for the computer system to limit individual user access rights only to the functions necessary to fulfill their job responsibilities. Such access controls prevent users from being involved in multiple aspects of financial transactions and restricts unauthorized access that can lead to the intentional or unintentional change or destruction of financial data. When it is impractical to segregate incompatible duties, District officials must provide oversight of the work being performed to mitigate the risk created by the incompatible duties.

Remote access is the ability to access a network from the internet or other external source. It must be controlled and monitored so that only authorized individuals can use the District's computer system or retrieve data. District officials should establish policies and procedures that address how remote access is granted, who is given remote access and how remote access will be monitored and controlled. If remote access users are not District employees, but are instead IT consultants, District officials should establish service level agreements (SLA) with these consultants regarding expectations and consequences for violating such expectations. An SLA should clearly stipulate the contract period, the services to be provided, measurable targets of performance and the basis for compensation.

District officials should have policies in place that address data protection issues such as protection of the District's computer network from viruses and malware, disposal of electronic hardware which may have stored personal or sensitive data, and access to data stored "in the cloud".

The District's information technology policies and procedure must be reviewed periodically and evolve with new developments in technology.

Information Technology (IT) Environment

Objective

Develop a knowledge base which represents the District's understanding and implementation of the data protection policies and procedures as is applicable to the information technology department's management of electronic data systems and devices.

Procedures

A detailed list of questions was developed to assess the existing policies and procedures currently in effect within the District with regard to the implementation of information technology within the District as it relates to the protection of data. The questions were developed to determine if common and best practices were employed in the District's IT environment.

Interviews and inquiries were conducted with the District's Director of Technology, Michael Tudisco. The "findings" presented are based on the information provided by Michael Tudisco, District employees and the District's insurance agent. We have not performed any tests to determine the validity of responses and information provided.

Findings

The following are the questions that were addressed by the District's Director of Technology. A synopsis of our findings is presented after each question.

- *Are there written policies and procedures relating to access rights, security, privacy rights, compliance with laws, retention period, method of disposal, etc. as related to the information technology environment? Please provide a copy.*

The District has Policy # 6470, adopted June 11, 2001, entitled "Staff Use of Computerized Information Resources" (see **Appendix D**) and related regulations. However, this policy and related regulations may not address the wide range of issues, responsibilities, and procedures that should be included in such a policy.

Recommendation:

We recommend that the District's Board of Education expand and update the policy to incorporate all relevant aspects of the District's information technology environment (network related systems, computer equipment, software, operating systems, storage media, mobile devices, network accounts providing electronic mail and/or resources, internet browsing, data breaches, emerging risks, etc.).

Information Technology

At a minimum, the policy should address the following:

- A comprehensive acceptable use policy, including guidelines and responsibilities
- Access security, including password policies and unattended computers
- Network security, including anti-virus software, firewall, data encryption, etc.
- Administrator rights
- Wi-fi access
- Sensitive and confidential information (and compliance with federal and state law)
- Transfer and storage of data
- Assignment and control of access rights
- Guest and vendor access
- User laptop and tablet policy (District owned)
- Use of personal mobile devices (laptops, tablets, smartphones) with District network
- Revocation of privileges
- Unacceptable use (including system/network activities, email and communications activities)
- Network administrator responsibilities (including network/data security, requests for support, continuing training, compliance with hardware and software licenses, notification of data breach or violations, management of system/software updates and patches)
- Response to security issues
- Monitoring of network activity through monitoring devices/applications such as firewall logs, web filtering logs, network traffic monitoring, active directory monitoring, mail scanner logs, backup and usage logs on servers, and event logs and histories created in individual machines
- Data loss prevention (includes data backup procedures)
- Technology committee

Information Technology

- Policy enforcement
- Response protocol in the event of a data breach
- Cyber insurance (to protect against losses/expenses related to data breaches)

A sample Information Technology Policy is presented at **Appendix E**.

- *Does the District have a Technology Committee, or similar working group, within the District?*

The District does have a Technology Committee.

- *Is the District's IT staff aware of any current data security risks?*

No.

- *Is there a formal procedure for handling reported security risks?*

There appears to be no formal written policy to handle data security risks/breaches or inappropriate use of network resources.

We were advised that there are informal procedures followed, as in the case of a student inappropriately using the District's network resources. If evidence is found that a student attempts to access unauthorized District data, the incident will typically be reported by a teacher or computer aid. The student will face disciplinary action – usually a suspension of technology privileges.

Recommendation:

We recommend that the District expand its IT policy to include a protocol for reporting security risks.

District Policy # 7314 "Student Use of Computerized Information Resources" addresses rules governing student use of computerized resources and related consequences for misuse.

- *Have there been any security breaches, or attempted security breaches, in the District?*

Last year, a student brought a flash drive with packet sniffing software and other tools (designed to read and manipulate information sent across the network) to school. The student proceeded to discover the wireless network SSID (wireless network name) and

crack the wireless network encryption. Upon discovery, IT removed the compromised SSID and the student had his internet privileges revoked for a few weeks.

Information Technology

No information was stolen because the wireless network cannot communicate with privileged systems. There have been no known instances of a data breach initiated by administrators or other privileged staff.

- *Does the District have a data breach policy?*

No.

Recommendation:

We recommend that the District develop a comprehensive IT policy that includes procedures to identify, document (preserve evidence), and report a data breach, a process to notify all those whose data was affected, a process to determine how the breach occurred and how to prevent a reoccurrence.

Recommendation:

A data breach can be very costly. The District's current general liability insurance policy with New York Schools Insurance Reciprocal (NYSIR) provides for limited protection. In response to the emerging data breach risk, NYSIR added a Personal Injury Extension Endorsement to its general liability policy, effective July 1, 2010. This has provided some third party liability coverage with respect to misappropriation of personal identification information when that misappropriation has resulted in the wrongful or fraudulent use of such information. This includes misappropriation through a breach of District information technology equipment.

There are relatively new insurance products available that are specifically designed to provide more comprehensive coverage in the event of a data breach, protections that the current NYSIR policies do not provide. This type of policy is called "Cyber Insurance".

Our recommendation would be to explore the cost/benefits of purchasing a "cyber insurance" policy.

Besides insurance protection, a "cyber insurance" policy can provide additional benefits when there is a data breach. These include:

- Forensic costs to examine the factors that led to the breach
- Costs to secure the site of the breach
- Costs to notify persons whose private information may have been breached and credit monitoring and call-center services for those persons

Information Technology

- Crisis management services (provided by law firms, public relations firms, breach response firms, and others) related to the breach, including costs to understand, evaluate, respond to, and communicate with regulators and the public
- *Is there a procedure to document and report a data breach incident to the Superintendent and Board of Education?*

No. There is no formal policy or procedure. The Director of Technology has indicated that if a data breach occurred, he would report the incident to Assistant Superintendent, Sam Gergis.

Recommendation:

We recommend that the District expand its IT policy to include a protocol for reporting a data breach to the Superintendent, Assistant Superintendent, and the Board of Education. The policy should also include procedures to notify those whose personal information was, or may have been, affected by the breach.

- *Is data backup adequate and is it tested periodically? / How are backups tested? / Is the backup data stored locally, in the cloud, or both? / How is the backup data protected from data theft?*

The backup process is deemed to be adequate. Integrity checks are run on the backup data to be sure that no corruption has occurred. The IT staff run periodic test restores of data on a random basis.

The backup data is stored both locally and in the cloud. Mission critical data is backed up on Acronis' servers (Acronis is a backup and data recovery service provider). Offsite data is encrypted on Acronis' servers. Other user data is backed up to disk on a daily basis using Symantec Backup Exec.

Protection from data theft is ensured by using data encryption for backup data stored in the cloud. The local backup data is stored in locked closets and is protected by Windows Authentication, Active Directory security groups, and NTFS security (NTFS/New Technology File System controls access to data files through the use of permissions for directories and/or individual files). It should be noted that the local backups are not encrypted.

Recommendation:

We recommend that the District consider using data encryption for local backups. Although the physical security of the local backups is adequate, if the backups were

physically accessed by intruders, it's fairly easy to circumvent the NTFS security safeguards.

Information Technology

- *Can backup data be restored in a timely manner if needed?*

Yes. Michael Tudisco estimates it would take two hours to restore the critical data from the Acronis servers.

- *By what means is network security assured?*
 - Switches and other network equipment are password protected.
 - Use of Cisco hardware with built in access control policies.
 - Access to most network equipment is restricted to certain IP addresses; one must sign into a specific switch to access the others.
 - Network configuration is handled by an outside company.
 - Separate networks using Virtual Local Area Networks to control which devices can communicate with one another. Data is separate from voice, which is separate from security. Student and Administrative data are on the same VLAN.
 - Separate Student and Administrative domains.
 - A trust relationship exists, but it's heavily restricted using Group Policy Objects (GPO).
 - Firewall
 - Utilize Symantec Endpoint Protection for Anti Virus (AV).
 - Utilize Windows Active Directory for Authentication.
 - Password policies in place.
- *With regard to the District's wireless network, what encryption method is used?*

WPA-TKIP

Recommendation:

Because WPA-TKIP encryption has been compromised, we would recommend using WPA2 encryption.

Note: The Director of Technology had indicated that most security related incidents involved students trying to gain access to the District's wi-fi. Using a higher standard of encryption should reduce these attempts.

Information Technology

- *Can sensitive data be accessed directly through the District's wireless network?*

No.

- *What precautions are in place for risks related to removable media, such as CD's or flash drives?*

BIOS is locked and password protected. Booting a computer from CD's or flash drives is disabled through BIOS.

Recommendations:

- Disable the "autorun" capability on all devices.
- Ensure that all removable media is scanned when mounted.
- Consider encrypting flash drives and other mobile devices. Encryption will keep data secure in the event of the loss of hardware like a laptop, iPad or flash drive. An added security step would be to make such drives "read only".
- *How is online transaction security ensured?*

In eSchool software Secure Sockets Layers (SSL) connections are used to create a secure connection between the District and the server.

With regard to banking transactions, all activity is encrypted by the banks.

- *Does the District use web-based applications?*

The District uses the following web-based applications:

- STAC online System (EFRT) - System to Track and Account for Children
- NYBEAS - the New York Benefits Eligibility and Accounting System - used for NYSHIP enrollment
- AESOP - absence management software
- eBoard - website creation for teachers
- IEP Direct - BOCES student information system for special education

- eSchool - run by CCSI

Information Technology

- *How is data security assured with regard to the District's web-based applications?*

The Director of Technology feels comfortable with the vendors' assurances of data security.

Recommendation:

We suggest that the District always obtain written assurances from each web-based application vendor that effective data protection safeguards have been implemented. Inquiries should be made to determine what level of liability these vendors are assuming for potential data breaches.

We performed online searches for the data protection policies of the providers of the District's web-based applications. A summary of their policies and safeguards, as presented on their websites, follows: (Please note that STAC and NYBEAS are administered by New York State - no statements of their safeguards could be found online).

- Aesop:

Security

The security of your user data is of utmost concern to us. In order to ensure that this data is completely protected and that your users can interact with our system in a secure fashion, the AESOP Systems has incorporated numerous security mechanisms and methodologies.

Security Components

Firewall. The AESOP System is shielded from intrusion by a system of enterprise-level firewalls. These firewalls ensure that the sensitive components of the AESOP System are completely invisible to the "outside world", while allowing only appropriate traffic to pass.

Intrusion Detection. All Internet traffic is thoroughly examined by an enterprise-level Intrusion Detection System (IDS). This system is managed and monitored by a team of highly skilled ecommerce security experts who will react to any suspicious activity immediately.

Encryption. AESOP web site access is secured using 56-bit Secure Socket Layer encryption. This ensures that all web interaction is completely protected from unwanted observation.

Information Technology

Security Methodologies

Industry Standard Security. The AESOP Infrastructure has been engineered to meet the most stringent security standards. All external administrative access is secured via a Virtual Private Network. Additionally, all access to the AESOP System is logged and audited on a regular basis.

E-commerce security expertise. FrontLine Data, Inc. retains the services of highly skilled ecommerce security experts. The expertise of these security specialists is used to validate AESOP System architecture and methodologies. Additionally, the security personnel can be dispatched to immediately address any security breach incident.

- eBoard:

eBoard is a basic webhost for teacher lesson plans, homework and lunch menus. No important or sensitive data is included (or should be) so no security requirement or audit exists. Data security isn't an issue with message boards.

- IEP Direct:

SIF Certified: The objective of the SIF Association is to enable disparate vendor applications to exchange data, without the end-user re-entering data multiple times, to provide secure and consistent information to all applications across a given environment. Checklists for the certification can be found at <http://cert.sifassociation.org/SitePages/Home.aspx>

VeriSign Secured: VeriSign Secured Seal which is now known as the Symantec seal is stamped on websites using secured and up to date SSL Certificates.

Microsoft Gold Certified Partner: Gold competencies demonstrate best-in-class capability within a specific Microsoft solution area.
<https://mspartner.microsoft.com/en/us/Pages/Membership/competencies.aspx>

Keeping private records private -

These days it's more important than ever to have the highest level of security when using a web-based application. That's why IEP Direct-New York uses state-of-the-art security technology to assure that private records remain private. Here are the features IEP Direct provides to prevent any compromise of your data:

128-bit SSL-encryption technology - the same top level of security relied upon by banks and other major financial institutions.

Information Technology

Customizable security levels - set access levels for individual students or groups - and control security at the document or function level.

No page caching - this ensures that identifiable student information never resides on a user's computer. All records remain secure at the IEP Direct website and any authorized district databanks.

Secure IEP files - finalized IEPs are encrypted and password-protected.

- eSchool:

eSchool commitment to data privacy and protection is assured by its issuance of an AICPA "SOC 3" report. SOC 3 (Service Organization Controls) reports are designed to meet the needs of users who want assurance on the controls at a service organization related to security, availability, processing integrity, confidentiality, and privacy.

It should be noted that the District's insurance agent has indicated that the District's current general liability policy provides some level of 3rd party liability coverage for incidents resulting in the misappropriation of personal information. Additional coverage can be secured through the purchase of a "cyber insurance" policy.

- *How is access to electronic data controlled?*

Through authorizations granted to appropriate/authorized District personnel. Authorized personnel are given login credentials (username and password) for the applications for which the employee needs access to fulfill his/her job responsibilities.

- *Does the District utilize data encryption (file-based encryption) for laptops, iPads and other external devices, secure network protocols for remote connections and website certificates? / Are client drives and server drives encrypted?*

No encryption is used for local files. Client drives and server drives are not encrypted.

Recommendation:

It is recommended that that all files (or entire disks) containing personal or sensitive data be encrypted. There is a common misconception that just requiring users to login to a device, or service, with a username and password provides an adequate level of protection for data. This isn't the case. In practice a password can be easily circumvented

and full access to the data can be achieved. Data encryption will provide a much higher level of security.

Encryption software uses a complex series of mathematical algorithms to protect and encrypt information. This hides the underlying data and prevents any inadvertent access

Information Technology

to, or unauthorized disclosure of, the information. This means that even if a device containing personal or sensitive information is lost or stolen, the information will remain secure as long as the would-be data thief isn't able to access the encryption key required to crack the algorithm.

Encryption software is widely available and a variety of encryption options are offered. The two primary options are 1) full disk encryption, and 2) individual file encryption.

Full disk encryption is a process which encrypts the entire disk including all of the information and personal data it contains. It is commonly used when encrypting laptops, desktops and mobile devices, such as mobile phone and tablets. The disk will need to be decrypted with a key, which is often protected by a password entered by the user, before the operating system boots up.

Individual file encryption is a process which will encrypt an individual file or create an encrypted container into which a set of files can be stored. When the container is closed it is encrypted. This means that if the container itself is transferred to a different device, for example if it is emailed or saved to a USB drive, then the personal data remains encrypted. However, once the file is removed from the container it is no longer encrypted.

- *What procedures are in place to secure data in transit?*

Secure Sockets Layer (SSL) certificates are employed.

SSL is an encrypted data transfer protocol. This is the technology that displays the padlock symbol in protected web browsing. It provides assurance that the communication between client and server cannot be intercepted. Furthermore it provides you with a means to validate where the data is being transferred to.

- *Is data properly classified and are access rights applied based upon the classifications?*

Yes. Organizational units and security groups are utilized.

- *May a person with appropriate rights to access the data, transfer the data to another device (for example, a flash drive)? If data may be transferred, what protections are in place to ensure that the data is secure on the secondary device?*

Yes, data may be transferred to another device. Once the data is transferred to another device it is not secured in any way.

Information Technology

Recommendation:

The current practice of allowing unsecured data to be transferred to other devices represents a significant risk. If the flash drive, laptop computer or iPad to which the data was transferred was lost, the unsecured data on the device is at risk of being misused.

We recommend that all personal or sensitive data, that may be copied or transferred to mobile devices, be encrypted. In the event that the mobile device was lost or stolen, the data would remain secured (unreadable).

- *Are there policies and procedures in place to be sure that authorizations for access to data are updated or removed as circumstances require (for example, employee terminations, employee retirements, and new employees)?*

There are no formal, written policies or procedures. The Director of Technology sets up network logins, email and special permissions as directed by the administration. Upon receiving notice of an employee termination or retirement, the login and email account is disabled.

Recommendation:

As discussed at the beginning of this section, we recommend that the District's policy be expanded to ensure that data access rights and procedures are properly administered and monitored.

- *Are user access logs maintained by the District?*

Yes, through iPrism and Finance Manager.

- *Are unnecessary client and server ports closed?*

Yes.

- *Are there any policies and procedures in place to protect unattended computer equipment?*

Yes. This is addressed in the regulations related to District Policy # 6470. It is the practice of the IT department to set computer monitors to lock if left idle. This is accomplished through settings in the group policies.

- *Is there a written District policy that specifies how long electronic records are to be retained?*

Information Technology

Yes. District Policy # 5670 "Records Management" sets forth the District's retention policy (based on New York State Schedule ED-1).

- *Is there a written District policy that specifies how records are to be disposed of?*

No.

Recommendation:

We recommend that the District develop a formal record retention policy that specifies how records (electronic and paper) are to be disposed of.

- *Is data removed from old equipment before disposal (for example, laptops, desktops, servers, mobile devices, and copiers)? If so, how is the data deleted?*

Yes. Data on all equipment is deleted using deletion tools such as Hiren's Boot CD.

- *What password policies are currently in place?*

There is no written District policy. However, the IT department has set up "group policies" that specifies password requirements.

Some software applications, such as Finance Manager and IEP Direct, have their own password requirements that must be adhered to. Finance Manager's passwords expire in thirty days. IEP Direct requires that passwords be reset at least once a year.

Recommendation:

We recommend that the District develop a formal policy for the use of passwords, password rules and expirations for access to personal or sensitive information. The policy should be periodically reviewed and updated to be responsive to the latest security threats.

It is a good practice to require strong, complex passwords which are changed regularly.

- *Is mobile computing permitted? If permitted, what safeguards are in place?*

Yes. It is permitted within District buildings, but blocked outside of buildings. Protection is provided through encryption on wi-fi. Also, SSID (Service Set Identifier) is not

broadcast. Hiding the SSID makes it more difficult for an unauthorized person to find the wireless network.

- *Is mobile device management used within the District?*

Information Technology

Yes. Airservers are used to manage District-owned iPads. District iPads are used for email only. Personal mobile devices are not managed and have no access.

- *Are internal voicemails protected by passwords?*

Yes. All voicemail is stored on a District server and can only be accessed by password.

- *Are District-created PDF files that contain personal or sensitive information password protected?*

No. The District does not password-protect any PDF files.

Recommendation:

We recommend that all PDF files that contain personal or sensitive information be encrypted (password protected).

- *How are systems containing personal or sensitive data kept separate from systems accessible by students and non-privileged staff?*

Sensitive data and student-accessible systems are maintained in separate domains.

- *What software controls are in place in the District?*

District Policy # 6470 and its related regulations address software controls to some degree. The IT Department denies administrator access for teachers and students. Other employees, such as administrators, have local administrator rights. All software installed on District computers/devices must be supplied by the District, but there is no District policy stating this.

Recommendation:

We recommend that administrative staff and anyone else who may have access to personal and sensitive data not be permitted to run their computers with local administrator rights.

We recommend that a formal software policy be developed.

We recommend setting up runtime controls, either through "whitelisting" approved software applications through Group Policy, or through other third party software. Whitelisting will allow only specified software to be installed and run on a computer.

We recommend a formal patch management schedule to ensure that software is secure and up to date.

Information Technology

- *Do District employees receive training in data security risks, security policies and procedures and best practices?*

Some do.

Recommendation:

It is advisable to provide periodic training/updates to employees regarding privacy, data protection and the District's policies. Reliance on technology alone to keep data safe is not enough. All data users need to be aware of the many risks and how to avoid them. Topics for training would include email safety, internet browsing safety, keeping personal data secure, procedures for reporting a data breach, and any other issues addressed in related District policy.

- *Is the District's email run on-site or hosted?*

Email is administered on-site using Microsoft Exchange.

- *Are email addresses publicly available?*

Yes, from the District's website.

Note: Publicly available email addresses is unavoidable in a public school environment. Spammers and hackers will have access to any publicly available email addresses.

- *Do email addresses match user login names?*

Yes.

Recommendation:

We recommend making email different from the login name. Using different names adds an additional layer of security from potential hackers (intruders). Hackers would need to guess both username and password, rather than just the password.

- *Are certain file types blocked as email attachments?*

No. No file types are blocked.

Recommendation:

We recommend that the following file types be blocked as email attachments: .bat, .chm, .cmd, .com, .cpl, .crt, .exe, .hlp, .hta, .inf, .ins, .isp, .jse, .lnk, .mdb, .ms, .pcd, .pif, .reg, .scr, .sct, .shs, .vb, and .ws

Information Technology

Allowing email attachments of these file types poses a significant risk to the District's network security as these file types can be used to imbed malicious code (viruses, Trojans, etc.) that can breach the District's data protections.

- *Are spam filters and virus scans applied to all incoming emails?*

Yes.

Privacy and Protection of Data - Business Office and Administration

Overview

The business office and administrative services provide support to all District schools and departments regarding budget, financial management, accounting, payroll, purchasing, transportation, security, safety, nutrition, and building and grounds.

All of the data risks discussed previously with regard to employee data, student data and information technology are present in the operations of the business office and administrative functions of the District. The business office, however, is subject to additional data risks related to its banking and investing activities.

Data security threats exist primarily when vulnerabilities exist in computer systems, software, or business practices. Most vulnerabilities are caused by out-of-date software, lack of security software (such as antivirus software, anti-spyware, etc.), weak authentication methods, or connecting to the Internet in a wide open manner (without a firewall between the user and the Internet.)

Development and adoption of effective policies and procedures that address the risks presented in previous sections of this report will address both the common and unique risks that exist in the business office and administrative services.

Business Office and Administration

Objective

Taking into consideration the functional components of both paper and electronic data, develop a knowledge base which represents the District's understanding and implementation of the data protection policies and procedures as is applicable to this area of records.

Procedures

Questionnaires were developed that addressed key areas of data maintained in both paper and electronic form. These questionnaires were sent to the individuals responsible for the following areas:

- Building and Equipment
- Accounting
- Banking
- Safety
- Security
- Transportation

Responses were compiled. Some respondents provided copies of documents to support/illustrate their replies. Follow-ups were conducted to clarify any responses received that were unclear or for which we determined additional information was necessary.

Findings

Section One - Preliminary and General Questions

Before addressing the actual records that contain administrative data, we made some inquiries pertaining to data protection in general. The following details those questions, along with our findings and recommendations.

- *Is the District insured against any claims arising from any violation of privacy laws, data breaches, etc.?*

The District's current general liability insurance policy with New York Schools Insurance Reciprocal (NYSIR) provides for limited protection. In response to the emerging data breach risk, NYSIR added a Personal Injury Extension Endorsement to its general liability policy, effective July 1, 2010.

Please refer to the IT section of this report for a discussion of additional protections offered by "cyber insurance" policies.

Business Office and Administration

Recommendation:

We recommend that the District evaluate the cost/benefit of acquiring cyber insurance to protect against the risks of data breach.

- *FERPA requires notification, disclosure and informed consent be made available to all parents. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of the district/school. Is this notification made at the District level or the school level? / Does the District have a policy pertaining to the student/parent directory? Please provide a copy. / Schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. How are these requests obtained and kept track of?*

The District's Policy #7240 Student Records addresses the FERPA requirement of notification in addition to the topic of directory information. The Office of the Superintendent issues a memo to the principals of each school in the District which provides the actual notification letter (both in English and in Spanish) and directs the principals to print the letter on the school's letterhead and send to the parents. (See **Appendix F**).

It also indicates the process whereby parents can request not to disclose directory information and states that such requests should be forwarded to Sam Gergis' office where they will be compiled and distributed to the appropriate District personnel.

It was indicated that this letter is also posted in the District Bulletin.

Recommendation:

None. FERPA notification requirements appear to be properly adhered to.

Section Two - Paper Records

Many of the same questions applicable to administrative paper records were asked in previous sections of this report and the same responses received. In order to avoid redundancy, the following are the questions posed for which it was deemed informative to present responses. If an issue was addressed in a previous section, our recommendation is not repeated here - reference is provided as to where it has already been cited in our report.

- *How are records disposed of/destroyed? / Who is accountable for its disposal/destruction?*

Business Office and Administration

Although a number of the respondents replied that they did not know the answers to these questions, it was stated that the records to be destroyed are identified by a building level administrator. Once identified, they are labeled and the Building and Grounds department is notified to contact the outside incinerator company and send records there.

Recommendation:

We recommend that a detailed, written policy be developed by the District to ensure that data is properly disposed of with assurances that no personal information is compromised in the process.

- *How are records secured (for example, locked cabinets)?*

A few of the respondents indicated either that their cabinets have no locks or the records with which they work are not locked.

Recommendation:

Please refer to Employee Data - Paper Records - same question.

- *Do you receive requests from third parties (non-employees of the District) seeking records? / Are there procedural guidelines to deal with requests for personal data from third parties?*

Most respondents acknowledged that they do receive third party requests. In addition, most were unaware of a formal policy/procedure or form to obtain before such requests were responded to.

District policies # 6420 "Employee Personnel Records and Release of Information" and # 7240 "Student Records" both address this issue and have been in place since 2001 and 2003, respectively.

Recommendation:

One respondent (as others in the Student Data section) provided a copy of the attachment to Regulation #7240R (see **Appendix G**). Although these forms are in existence, much of the personnel in the departments interviewed during this internal audit are unaware of them. We acknowledge that the District does have the appropriate policy in place, but

without communicating that policy to the appropriate personnel, it is essentially ineffective. It is recommended that all departments be provided with copies of these forms and instructed to use them as appropriate.

Business Office and Administration

Section Three - Electronic Records

Many of the same questions applicable to administrative electronic records were asked in previous sections of this report and the same responses received. In order to avoid redundancy, the following are the questions posed for which it was deemed informative to present responses.

If the question was addressed in a previous section, our recommendation is not repeated here - reference is provided as to where it has already been cited in our report.

- *How are rights to records established? / Are access rights updated periodically (for example, for employee terminations, retirements, new employees, etc.)? / How is access controlled?*

There was no clear answer as to how rights are established. We understand that rights are granted depending on position, necessity and sufficient internal control, but are unclear as to whether a policy exists or what the actual procedure is to determine the need and grant access to a file. It was noted that access is controlled by the Business Office and IT.

Recommendation:

We recommend that a detailed, written policy be developed by the District to ensure that data access rights and procedures are properly administered and monitored.

HUNTINGTON UNION FREE SCHOOL DISTRICT HUNTINGTON, NEW YORK 11743

I have received the following Board of Education Policies and Administrative Regulations for my review and compliance:

3231	Complaints and Grievances by Employees
3272	Staff Use of Laptop Computers
5230	Acceptance of Gifts, Grants & Bequests to the School District
5640	Smoking by Staff and Public
5665	Wellness Policy
5680	Safety and Security
5692	Human Immunodeficiency Virus (HIV) Related Illnesses
5800	Cellular Telephones
5800R	Cellular Telephones Regulations
6110	Code of Ethics
6111	Conflict of Interest
6112	Staff Student Relationships
6120	Equal Employment
6121	Sexual Harassment
6122	Non-Discrimination of Employees
6150	Alcohol, Drugs and Other Substances (School Personnel)
6151	Drug Free Workplace
6470	Staff Use of Computerized Information Resources
7350	Corporal Punishment
7530	Child Abuse
7531	Sexual Harassment of Students
7540	Suicide
7550	Racial Harassment (Students)
7570	Conditional Appointments
7580	Dignity for All Students Act
8130	Equal Education Opportunities
8220	Career (Occupational) Education

Please sign for, review and comply with the Policies and Regulations.

PLEASE PRINT YOUR NAME

PLEASE SIGN YOUR NAME

DATE

I:\Recruitment\District Policies Cover Sheet.doc

POLICY

2006

6110
1 of 2

Personnel

SUBJECT: CODE OF ETHICS FOR ALL DISTRICT PERSONNEL

Section 1. Pursuant to the provisions of Section 806 of the General Municipal Law, the Board of Education of the Huntington Union Free School District recognizes that there are rules of ethical conduct for members of the Board and employees of the District that must be observed if a high degree of moral conduct is to be obtained in our unit of local government. It is the purpose of this resolution to promulgate these rules of ethical conduct for the Board members and employees of the District. These rules shall serve as a guide for official conduct of the Board members and employees of the District. The rules of ethical conduct of this resolution, as adopted, shall not conflict with, but shall be in addition to any prohibition of Article Eighteen of the General Municipal Law or any other general or special law relating to ethical conduct and interest in contracts of Board members and employees.

Section 2. Standards of Conduct. Every Board member or employee of the Huntington Union Free School District shall be subject to and abide by the following standards of conduct:

(a) Gifts. An officer or employee shall not directly or indirectly solicit or accept any gift having a value of \$75 or more, whether in the form of money, services, loan, travel, entertainment, hospitality, thing or promise, or any other form, under circumstances in which it could reasonably be inferred that the gift was intended to influence him/her, or could reasonably be expected to influence him/her, in the performance of his/her official duties, or was intended as a reward for any official action on his/her part. No gift in any form shall be accepted that exceeds standards as established by all applicable municipal law.

★ (b) Confidential Information. He/she shall not disclose confidential information acquired by him/her in the course of his/her official duties or use such information to further his/her personal interest.

(c) Representation before one's own agency. He/she shall not receive, or enter into any agreement, express or implied, for compensation for services to be rendered in relation to any matter before any municipal agency of which he/she is an officer, member or employee or of any municipal agency over which he/she has jurisdiction or to which he/she has the power to appoint any member, officer or employee.

(d) Representation before any agency for a contingent fee. He/she shall not receive, or enter into any agreement, express or implied, for compensation for services to be rendered in relation to any matter before any agency of his/her municipality, whereby his/her compensation is to be dependent or contingent upon any action by such agency with respect to such matter, provided that this paragraph shall not prohibit the fixing at any time of fees based upon the reasonable value of services rendered.

(e) Disclosure of interest in resolution. To the extent that he/she knows thereof, a member of the Board of Education or employee of the Huntington Union Free School District, whether paid or unpaid, who participates in the discussion or gives official opinion to the Board of Education on any

HUNTINGTON UNION FREE SCHOOL DISTRICT
FOOD & NUTRITION DEPARTMENT

RETENTION OF RECORDS

DESCRIPTION OF RECORD

RETENTION

1.[135] Food Management and Child Nutrition Records

a. Program participation agreement, including Attachments and amendments:

6 years after termination of agreement

b. Other program records, including but not limited to application to participate as a sponsor, individual child participation application, records including meal counts, requisition and approval of requisition for donated commodities, and fiscal records such as adding machine tapes, purchase orders, claims and vouchers:

3 years after school fiscal year (3 years plus current year)

NOTE: Fiscal records relating to food management and child nutrition do not need to be retained for 6 years as similar fiscal records found in the Fiscal section of this schedule must be retained

c. Free and reduced meal policy statement, with attachments and certificate of acceptance:

3 years after policy superceded

2.[136] Food Inspection and Investigation Records

a. Inspection report for preparation or serving area

3 years

b. Food sanitation complaint investigation or food embargo records, for investigations **other than** food or water-borne disease investigations

6 years after last entry

c. Food sanitation complaint investigation or food embargo records, when a food or water-borne disease investigation is conducted.

21 years

NOTE: Appraise these records for long-term uses, warranting longer, if not permanent, retention prior to disposition. Records covered by item no. 136c may be useful in the future in documenting cases of serious food poisoning such as where death or serious illness occurs from E. coli contamination. Contact the State Archives for additional advice.

3. Paid bills

6 years after school fiscal year (six years plus current year)

4. Reimbursement Claim files (Director of Food and Nutrition wants all past and present files kept in current file drawer

HUNTINGTON UNION FREE SCHOOL DISTRICT

P.O. BOX 1500, Huntington, NY 11743

Registration Office 631-673-2974

RECORDS REQUEST

The student named below has registered in our school district. Kindly fax academic and health reports, including immunizations, to the school as indicated. A prompt response is greatly appreciated.

SCHOOL FAX NUMBER

___ Flower Hill Primary 631-425-6255	___ Abrams Intermediate 631-425-6256
___ Washington Primary 631-425-6259	___ Woodhull Intermediate 631-425-4718
___ Southdown Primary 631-425-6258	___ Finley Middle School 631-425-4746
___ Jefferson Primary 631-425-6257	___ Huntington HS 631-425-4730

STUDENT NAME _____ DATE OF BIRTH _____

Last Grade Attended _____

Former School Name _____

School Address _____

Town/State/Zip _____

Fax Number _____

PARENTAL PERMISSION:

I give my permission to release this information to the Huntington School District.

Parent/Guardian Signature _____ Date _____

Huntington Union Free School District
Washington Primary School
78 Whitson Rd.
Huntington Station, New York 11746

Phone (631) 673-2090

Fax (631) 425-6259

AUTHORIZATION FOR RELEASE OF INFORMATION

Date: _____

I hereby give my permission for the exchange of the following information/evaluations:

Educational, Psychological, Psychiatric, Medical, Neurological, Occupational Therapy, Physical Therapy, Speech Therapy, Social History and current IEP for _____ school year, Other _____

Between the:

Huntington Union Free School District
Washington Primary School
78 Whitson Road
Huntington Station, New York 11746

and _____

Fax #: _____

Phone #: _____

Regarding my child _____

DOB: _____

Parent/Guardian's Signature _____

Witness _____

Date Released/Mailed/Faxed (Initial) _____

Please note: This form is to be filled out and mailed by Student Support Services staff only.

cc: CSE File

Form Revised: 8/1/07

1a

HUNTINGTON UNION FREE SCHOOL DISTRICT
Huntington, New York

August 2013

**CONSENT TO RELEASE
FREE OR REDUCED PRICE ELIGIBILITY INFORMATION**

School officials may release information that shows that my child/children are eligible for free or reduced price meals to the following programs. I understand that the information will only be provided to the programs below:

- State or federal programs such as the Youth Summer Work Program;
- Local health and education programs and other local programs that provide benefits such as free band instruments, or reduced fees for summer school or driver education;
- Community summer arts and playground programs.

I understand that I will be releasing information that will show my child/children are eligible for free and reduced price meals or free milk for my child. I give up my rights to confidentiality for this program.

Child/Children

I certify that I am the parent/guardian of the child/children for whom the free/reduced price application was made:

Signature of Parent/Guardian:

Print Name:

Address:

Phone Number:

Date:

Huntington Union Free School District
Student Support Services Department
50 Tower Street
Huntington Station, New York 11746

Phone (631) 673-2115

Fax (631) 425-4727

AUTHORIZATION FOR RELEASE OF INFORMATION

Date: _____

I hereby give my permission for the exchange of the following information/evaluations:

Special Education: Social History, Educational, Psychological, Psychiatric, Functional Behavior Assessment, Behavior Intervention Plan, Medical (including immunizations), Neurological, Occupational Therapy, Physical Therapy, Speech Therapy, Prior Written Notice/Consent and IEP for the following school years: _____

General Education: Report Cards, Standardized Test Scores, Transcripts

Other: _____

Between: _____

Nancy Wilson
Director of Special Education & Student Support Services
Huntington Union Free School District
Student Support Services Department
50 Tower Street
Huntington Station, NY 11746

AND

Fax# _____

Phone# _____

Regarding my child _____ DOB: _____

Guardian's Signature _____

Guardian Print Name _____

Date Released/Mailed/Faxed (Initial) _____

cc: Student's CSE File

Updated: 2/24/2014 2:36 PM

7240F.1

**HUNTINGTON UNION FREE SCHOOL DISTRICT
AUTHORIZATION FOR RELEASE OF RECORDS**

I, _____, hereby authorize

the _____ to release copies
(name of school)

of _____
(list records)

which are part of the records of _____

and to furnish them to _____

for the purpose of _____

Signature

Date

This form must be signed by the parent/guardian or eligible student prior to the release of personally identifiable student information to a third party at the request of the parent/guardian or eligible student.)

POLICY

2001

6470
1 of 2

Personnel

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES

The Board of Education will provide staff with access to various computerized information resources through the District's computer system (DCS hereafter) consisting of software, hardware, computer networks and electronic communication systems. This may include access to electronic mail, so-called "on-line services" and the "Internet." It may also include the opportunity for some staff to have independent access to the DCS from their home or other remote locations. All use of the DCS, including independent use off school premises, shall be subject to this policy and accompanying regulations.

The Board encourages staff to make use of the DCS to explore educational topics, conduct research and contact others in the educational world. The Board anticipates that staff access to various computerized information resources will both expedite and enhance the performance of tasks associated with their positions and assignments. Toward that end, the Board directs the Superintendent or his/her designee(s) to provide staff with training in the proper and effective use of the DCS.

Staff use of the DCS is conditioned upon written agreement by the staff member that use of the DCS will conform to the requirements of this policy and any regulations adopted to insure acceptable use of the DCS. All such agreements shall be kept on file in the District office.

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance shall apply to use of the DCS. Employees are expected to communicate in a professional manner consistent with applicable District policies and regulations governing the behavior of school staff. Electronic mail and tele-communications are not to be utilized to share confidential information about students or other employees.

This policy does not attempt to articulate all required and/or acceptable uses of the DCS; nor is it the intention of this policy to define all inappropriate usage. Administrative regulations will further define general guidelines of appropriate staff conduct and use as well as proscribed behavior.

District staff shall also adhere to the laws, policies and rules governing computers including, but not limited to, copyright laws, rights of software publishers, license agreements, and rights of privacy created by federal and state law.

Staff members who engage in unacceptable use may lose access to the DCS and may be subject to further discipline under the law and in accordance with applicable collective bargaining agreements. Legal action may be initiated against a staff member who willfully, maliciously or unlawfully damages or destroys property of the District.

(Continued)

POLICY

2001

6470
2 of 2

Personnel

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES (Cont'd.)

Privacy Rights

Staff data files and electronic storage areas shall remain District property, subject to District control and inspection. The Director of Technology may access all such files and communications to insure system integrity and that users are complying with requirements of this policy and accompanying regulations. Staff should NOT expect that information stored on the DCS will be private.

Implementation

Administrative regulations will be developed to implement the terms of this policy, addressing general parameters of acceptable staff conduct as well as prohibited activities so as to provide appropriate guidelines for employee use of the DCS.

Adopted: 6/11/01

Information Technology Policies and Procedures

X School District

June 1, 2014

TABLE OF CONTENTS

TABLE OF CONTENTS..... 1

1.0 OVERVIEW..... 2

2.0 PURPOSE 2

3.0 SCOPE..... 2

4.0 ACCEPTABLE USE POLICY 2

 4.1 GENERAL USE AND OWNERSHIP..... 2

 4.2 SECURITY 4.2.1 PASSWORDS, ACCOUNTS, AND ANTIVIRUS 3

 4.2.2 Network Security and Administrator Rights..... 3

 4.3 SENSITIVE AND CONFIDENTIAL INFORMATION 3

 4.3.1 Definition and Protection 3

 4.3.2 Access and End User Support 4

 4.4 GUEST AND VENDOR ACCESS 4

 4.5 USER LAPTOP POLICY 4

 4.6 REVOCATION OF PRIVILEGES 5

5.0 UNACCEPTABLE USE..... 5

 5.1 UNACCEPTABLE USE: SYSTEM AND NETWORK ACTIVITIES..... 5

 5.2 UNACCEPTABLE USE: EMAIL AND COMMUNICATIONS ACTIVITIES 6

6.0 NETWORK ADMINISTRATOR RESPONSIBILITIES..... 6

7.0 SECURITY INCIDENTS 7

 7.1 DEFINITION 7

 7.2 RESPONSE 8

 7.3 MONITORING..... 8

 7.3.1 Devices and Applications 8

 7.3.2 Files and Correspondence 8

8.0 DATA LOSS PREVENTION 9

9.0 PURCHASING 9

10.0 TECHNOLOGY COMMITTEE 9

11.0 ENFORCEMENT 10

12.0 REVISIONS..... 10

APPENDIX A..... 11

APPENDIX B..... 12

APPENDIX C 13

APPENDIX D 15

1.0 Overview

The IT Department's intention for publishing Policies and Procedures is not to impose restrictions that are contrary to X School District's established mission of providing users with the best tools possible to educate every student. Rather the IT Department is committed to protecting X School District's users from illegal or damaging actions by individuals, either knowingly or unknowingly. Network related systems, including but not limited to computer equipment, software, operating systems, storage media, mobile devices, network accounts providing electronic mail and or resources, WWW browsing, and FTP, are the property of X School District. These systems are to be used for educational and school business-related purposes with the intent of serving the interests of the students, teachers, and other staff members of X School District. Maintaining a network requires proper planning, organization, monitoring, and effective security. A team effort involving the participation and support of every X School District employee and affiliate is required to meet and exceed the standards set forth by New York State Law, Federal Law, and the X School District's Board of Education and administrators. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of the network-related systems within the X School District. These rules are in place to protect the students, staff, and the X School District. Inappropriate use, improper planning, and disregard of these procedures exposes X School District to risks including compromise of network systems and services, possible damage to the network, and legal issues.

3.0 Scope

This policy applies to students, employees, contractors, consultants, temporaries, authorized guests, and other workers at X School District, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by X School District to include all future purchases.

4.0 Acceptable Use Policy

4.1 General Use and Ownership

- Users should be aware that the data they create on the network remains the property of X School District. Users should have no expectations of expressed or implied privacy.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Network/Internet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- Using the X School District network is a privilege. As with all privileges, it is the responsibility of the guest user to use this service appropriately and in compliance with all school board policies and procedures, New York State law, and Federal laws.
- The use of excessive bandwidth and reproduction of copyrighted materials is strictly forbidden and will result in the termination of network services.
- The X School District assumes no responsibility for costs associated with loss or damage to devices not owned by X School District while on the network.
- For security and network maintenance purposes, the IT Department may monitor equipment, systems, and network traffic at any time.

- The X School District's IT Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security

4.2.1 Passwords, Accounts, and Antivirus

- Users, which includes employees, students, and guests of X School District, will be granted access to the network after they have signed the appropriate Network Usage Agreements forms (see Appendix A, Appendix C, and Appendix D).
- Users must keep passwords secure and are not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Users shall not leave computer unattended while logged on.
- Users of Windows based computer's will be required to change their passwords every 60 days as prompted automatically by Windows Active Directory.
- Users needing password resets for various programs must contact the IT Department. Every attempt will be made to identify the user by positive identification. This method may include sight/voice reconciliation, a predetermined security question, or other questions as determined by the Director of Technology.
- All computers used by students, employees, or guests that are connected to the X School's network, whether owned by the user or X School District, shall be continually executing virus-scanning software with a current virus database.
- Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.2.2 Network Security and Administrator Rights

- Administrative passwords for the network, servers, computers, wireless access points, and other electronic devices are to be kept strictly confidential and known only by the IT staff members that need them to perform their duties. Distributing passwords of any kind is strictly forbidden.
- Wireless access points will be secured with a security mechanism to be determined by the IT Director. The wireless security code will be entered into authorized devices by the IT staff only. Any attempt to obtain and/or distribute this code is strictly forbidden.
- Users using X School District devices will not be granted Administrative Rights to those devices unless they submit a written request to the IT Department proving that they have a legitimate need for such rights. The IT Director and/or IT staff will determine if there is another alternative before granting such rights.

4.3 Sensitive and Confidential Information

4.3.1 Definition and Protection

When handling sensitive and confidential information, precautions must be taken to prevent unauthorized access to the information. Staff members may not disclose sensitive information to persons not authorized to receive it. This includes non-public information such as Social Security Numbers, credit card numbers, bank account numbers, health information, or other confidential student and user data.

All users who have access to or may have access to personally identifiable student and user records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), X School Board Policies and Procedures, and all other applicable State and Federal laws and regulations, as they relate to the release of such information.

Below are the guidelines that must be followed where applicable:

- Encrypt data.
- Password protect data.
- Physically protect devices that can be easily moved such as PDA and Laptops that are used to access sensitive data.
- Avoid creating files that use social security numbers as identifiers. Use employee numbers and/or student local identification number instead.
- Never download or copy sensitive data to your home computer
- Never store un-encrypted data on a portable device
- Protect printed sensitive data. Store sensitive data in locked desk, drawer or cabinet. Do not leave unattended sensitive data on copier, FAX, or printer. Shred sensitive data that need to be disposed.

4.3.2 Access and End User Support

Sensitive data access is restricted to only those personnel who need to perform their job duties. Access restrictions to such data are maintained by the IT Department in conjunction with the Finance Department, the Human Resources Department, the Superintendent of X School District, and the School Board. Accesses to sensitive information are only granted at the request of an administrator with an accompanying and verifiable need.

Reviews of accesses and privileges are conducted regularly and monitored to ensure compliance with all School Board Policies as well as State and Federal Laws and regulations.

See Appendix E

4.4 Guest and Vendor Access

- Guest and Vendor access will not be granted to any X School District network or network device without a signed and approved vendor contract or a Guest Access Agreement Form (Appendix D).
- Using the X School District network is a privilege. As with all privileges, it is the responsibility of the guest user to use this service appropriately and in compliance with all school board policies and procedures, New York State law, and Federal laws.
- The use of excessive bandwidth and reproduction of copyrighted materials is strictly forbidden and will result in the termination of network services.
- The X School District assumes no responsibility for costs associated with loss or damage to devices not owned by X School District while on the network.
- The X School District IT staff can provide limited support in aspects of network connectivity and access of network resources.
- Backing up data and ensuring the security of network devices are the sole responsibility of the owner.
- Vendor supplied user ID's, program passwords, guest accounts, and security devices are administered by the IT Department. This information and these devices are kept secure from general users unless knowledge of them is imperative to the course of their job.

4.5 User Laptop Policy

- Users that are issued laptops by the X School District must sign a Laptop Usage Agreement form upon receipt of the laptop (see Appendix B).
- Users will be responsible for the security of the laptop while assigned to them whether on or off campus.

- Users must understand that issued laptops are property of X School District and shall be returned in their original condition upon request.
- Users assume all risk of injury or harm associated with the use of the laptop off-premises, including but not limited to, physical damage or loss, or personal injury.
- While laptops are being used off campus, the X School District has no control over the information accessed through the Internet and cannot be held responsible for content viewed.
- X School District and its users will not be held liable for claims for damages that may arise from the use of issued laptops while not on school property.

4.6 Revocation of privileges

Privileges and accesses to all X School District network devices, software, email, and information systems will be revised or revoked as necessary in the event of the following

- Transfer of employee
- Resignation of employee
- Termination of employee
- Termination of vendor contract.
- Termination of consulting contract
- In the event of an investigation of employee, vendor, or consultant where revision or revocation of privileges and access is necessary.

5.1 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host, if that host is disrupting production services).

- Under no circumstances is an employee, student, or authorized guest of X School District authorized to engage in any activity that is illegal under local, state, federal or international law, while utilizing X School-owned resources, to include the network and Internet.
- Users shall not access, download, store, send, or display text, images, movies, or sounds that contain pornography, obscenity, or language that offends or degrades others.
- Attempts to circumvent or defeat mechanisms put in place by the X School District staff to manage the network is strictly forbidden.
- Users shall not attempt to download and/or install services, electronic file sharing mechanisms, games, software, tools, or any executable file.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

5.1 Unacceptable Use: System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by X School District.

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which X School District or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a X School District computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any X School District account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning unless prior notification and approval is received beforehand.
- Executing any form of network monitoring unless prior notification and approval is received beforehand.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the user's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the network/Internet.
- Providing information about, or lists of, X School District's users to parties outside the X School District without prior permission from the Superintendent.

5.2 Unacceptable Use: Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Students shall not use social network sites including, but not limited to, myspace.com, facebook.com, chat rooms, etc.
- Students shall not agree to meet with anyone met online.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within X School District's networks or other Internet/network service providers on behalf of, or to advertise, any service hosted by X School District or connected via X School District's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

6.1 Network Administrator Responsibilities

It is the responsibility of the network administrator to follow the guidelines and policies of the Director of Technology, X School District, New York State Department of Education, and all State and Federal Laws.

Network Administrators report to the Director of Technology. Regular meetings, as determined by the Directory of Technology, are to be held between the Network Administrators and the Director and Assistant Director of Technology in order to maintain close working relationships and openness in day-to-day communications.

Among their other responsibilities, the Network Administrator should use reasonable efforts to:

- Respond to requests for support, information, problem determination and problem resolution.
- Become familiar with all applicable X School District IT policies.
- Participate in required Network Administrator training and regular meetings as determined by the Director of Technology.
- Take precautions against theft of or damage to the system components and information.
- Comply with terms of all hardware and software licensing agreements applicable to the system.
- Treat information about, and information stored by, the network users in an appropriate manner and to take precautions protecting the security of the network and the security and confidentiality of the information contained therein.
- Promptly inform the Director and/or Assistant Director of Technology of any computing incidents which clearly compromise network integrity, including but not limited to:
 - Notification by outside institutions or individuals of any incident.
 - Data loss or theft.
 - Inappropriate systems or information access or use
 - Any other breach or violation of IT policies of which they become aware.
- Promptly notify the Director and/or Assistant Director of material changes in network architecture or administration.

Network Administrators, when requested, are expected to cooperate fully with the Director of Technology in any investigation, identification, and resolution of network incidents.

Network Administrators are not responsible for the content of files, images, video or audio clips, electronic communications, and news postings produced by others. The Network Administrator is also not responsible for unauthorized software installed by others. Network Administrators are responsible, however, for notifying the Director of Technology of any observed violations of X School District policies, licensing agreements with software manufacturers, or observed violations of local, state, or federal laws regarding these matters.

7.0 Security Incidents

7.1 Definition

A security incident is any violation of set Policies and Procedures that may or may not result in the following:

- loss of information confidentiality (data theft)
- compromise of information integrity (damage to data or unauthorized modification)
- theft of physical IT asset including computers, storage devices, printers, etc.
- denial of service
- misuse of services, information, or assets
- infection of systems by unauthorized or hostile software
- an attempt at unauthorized access
- unauthorized changes to organizational hardware, software, or configuration

- reports of unusual system behavior etc

7.2 Response

If a Network Administrator becomes aware of a security incident, they must provide notification of the incident to the Director of Technology. Upon confirmation, the Director of Technology will notify the user's supervisor (if a X School District employee) or School Administrator (if a X School District student).

Other steps that may be taken:

- Temporarily suspend or restrict the user's computing privileges during the investigation.
Reactivation is at the discretion of the Director of Technology.
- Remove the affected computer device, as appropriate, from the network.

These steps may be taken only after authorization by the Director of Technology unless the situation represents an emergency or immediate threat to network security/integrity. In such case, the Network Administrator must take corrective action and notify the Director of Technology as soon as possible. Actions should be taken in such a way that any impacts to non-offending users are minimized.

7.3 Monitoring

7.3.1 Devices and Applications

In effort to maintain network security, integrity, and to reduce the risk of Security Incidents the IT Department, at the discretion of the Director of Technology, can and will monitor network activity. These monitoring devices/applications include but are not limited to:

- Firewall logs
- Web Filtering logs
- Network Traffic Monitoring
- Active Directory Monitoring
- Mail Scanner logs
- Database, backup, and usage logs on servers
- Event logs and histories created in individual machines

7.3.2 Files and Correspondence

In the course of their duties, it may be necessary for Network Administrators to view files, data or communications that have been stored by users on devices or network file servers. The viewing of such material is permitted only when it is necessary to troubleshoot problems at the request of the user, protect the security and integrity of the X School District's network, protect the rights or property of X School District or third parties, or to ensure compliance with X School District policy or applicable law. Examples include:

- the identification/restoration of lost, damaged or deleted files;
- the identification of a process that is interfering with normal network functions;
- or, in more serious circumstances, an investigation of a Security Incident.

In all such cases, the Network Administrator shall take into consideration the confidential nature of files and/or communications that may potentially be reviewed and shall implement the appropriate safeguards to ensure that all local, state and federal privacy laws are complied with. The Director of Technology must be advised of and approve any non-routine monitoring that occurs. Non-routine monitoring includes directed investigations of potential policy and/or security violations. Discovery of such violations in the course of routine monitoring must be reported.

8.1 Data Loss Prevention

To prevent data loss from a disaster, the IT Department will follow all disaster policies and guidelines set forth by the X School District. In addition, the IT Department will take routine measures to protect and restore critical on-site systems by performing daily, weekly and monthly backups and storing backups in three separate and secure locations. Contacts for information systems off-site include data loss protection plans and disaster recovery plans as a rule before approval.

In the event of immediate threat the IT Department will take the following actions:

- Backups will be performed and stored in all three locations if possible
- Most servers except First Class E-mail will be shut down.
- The generator will be started if needed for power.
- Information will be provided on the X School District web site.
- Network closets and battery backups (UPS) should be turned off if unnecessary
- In the event the MIS building is damaged or destroyed, operations will be re-established at one of the schools or department buildings.

Each school and district office department should take the following steps to protect data and equipment:

- Computers should be turned off and unplugged, if connected to battery backups there should be turned off and unplugged as well.
- Computers should be moved away from windows, off the floor, and covered with plastic if possible.

9.0 Purchasing

The IT department is responsible for the seamless integration of any hardware or software into the existing network system and maintaining an inventory of all such items. When considering the purchase of any technology related item, prior approval from the IT Department is required. Procedures to obtain approval for purchase of technology equipment are determined by the Finance Department. A verbal request is not acceptable. In addition, a quote for purchases is not an approval for purchase.

10.1 Technology Committee

The X School District will maintain a Technology Committee comprised of the IT Director, Assistant IT Director, other IT staff as necessary, District level Administrators, and one administrator and one faculty member from each school.

The Purpose of the Technology Committee is:

- To provide a forum to discuss issues, concerns, and/or interests of the teachers and administrators at each school with the IT Department.
- To assist in promoting the efficient use of technology in schools, including creating standards for the management and application of technology.
- To serve as a resource for X Schools in helping all users understand technology in schools and how to use it properly and efficiently.
- Assist in planning for and evaluating classroom technology (such as model classrooms and educational software).
- Assist in planning professional development activities related to technology.
- Assist in other activities as deemed appropriate by the committee in collaboration with the IT Department and Superintendent.

11.0 Enforcement

Failure to adhere to these policies and guidelines may result in suspension or revocation of the offender's privilege or access to the network and/or other disciplinary or legal action.

12.0 Revisions

The X School District reserves the right to change these policies and procedures at any time to ensure the operability and safety of the network and its users.

HUNTINGTON UNION FREE SCHOOL DISTRICT
Office of the Superintendent

Memo To: Principals
From: James Polansky
Date: August 19, 2013
Subject: **NCLB - Notification of Rights Under FERPA**

Attached you will find the Notification of Rights Under Family Education Act (FERPA) and Privacy Act and No Child Left Behind Act of 2001. Please prepare and send this notification to your parents within the first 1 - 2 weeks of school. Also attached is Policy 7240 - Student Records. The policy is for your information, not distribution.

As indicated in the notice, parents who do not want the district to disclose any directory information must notify their principal in writing by September 27th. Principals must then insure their request is granted. In addition, please copy and forward all requests to Sam Gergis's office. Mr. Gergis will compile and distribute the information to the appropriate district-wide personnel.

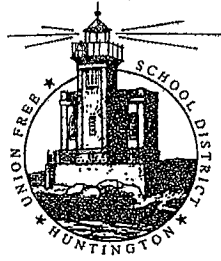
Thank you for your anticipated cooperation. If you have any questions please call me.

att: FERPA Notice, English
FERPA Notice, Spanish
Policy 7240 - Student Records

cc: Kenneth Card
Sam Gergis
Directors
Chairs

JP:mc
Encl.

Ferpa-NCLC Principal Memo



Flower Hill Primary School

"A Tradition of Excellence Since 1657"

Mr. Marlon C. Small
Principal

September, 2013

Dear Parents/Guardians:

Attached please find a copy of the Notification of Rights under the Family Educational Rights and Privacy Act (FERPA) and the No Child Left Behind Act of 2001. FERPA affords both parents and students over eighteen years of age certain rights with respect to the student's education records. One of these rights is the right to consent to disclosures of personally identifiable information contained in the student's educational records.

FERPA also permits the district to disclose appropriately designated "directory information" without written consent, unless parents or eligible students have advised the school not to do so. If you do not want the district to disclose any or all directory information from your child's education records without your prior written consent, you must notify the district in writing. Please send your letter to me at Flower Hill School by Friday, September 27, 2013.

If you have any questions or concerns regarding this matter, please call the school at 673-2050. Thank you in advance for your anticipated cooperation.

Sincerely,

Marlon C. Small
Principal

Huntington Union Free School District
"A Tradition of Excellence Since 1657"

Notification of Rights under Family Educational Rights and Privacy Act
and No Child Left Behind Act of 2001

The Family Educational Rights and Privacy Act (FERPA) affords parents and students over 18 years of age or students attending an institution of post-secondary education ("eligible students") certain rights with respect to the student's education records. These rights are:

1. The right to inspect and review the student's education records within 45 days of the day the School receives a request for access. Parents or eligible students should submit to the student's Building Principal a written request that identifies the record(s) they wish to inspect. The Building Principal will make arrangements for access and notify the parent or eligible student of the time and place where the records may be inspected.
2. The right to request the amendment of the student's education records that the parent or eligible student believes are inaccurate or misleading. Parents or eligible students may ask the School to amend a record that they believe is inaccurate or misleading. They should write the student's Building Principal, clearly identify the part of the record they want changed, and specify why it is inaccurate or misleading. If the School decides not to amend the record as requested by the parent or eligible student, the School will notify the parent or eligible student of the decision and advise them of their right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the parent or eligible student when notified of the right to a hearing.
3. The right to privacy of personally identifiable information in the student's education records, except to the extent that FERPA authorizes disclosure without consent. One exception, which permits disclosure without consent, is disclosure to school officials with legitimate educational interests. A school official is a person employed by the School as an administrator, supervisor, instructor, or support staff member (including health or medical staff and law enforcement unit personnel); a person serving on the School Board; a person or company with whom the School has outsourced services or functions it would otherwise use its own employees to perform (such as an attorney, auditor, medical consultant, or therapist); a parent or student serving on an official committee, such as a disciplinary or grievance committee; or a parent, student, or other volunteer assisting another school official in performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility. Upon request, the School discloses education records without consent to officials of another school district in which a student seeks or intends to enroll, or is already enrolled if the disclosure is for purposes of the student's enrollment or transfer.
4. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the School to comply with the requirements of FERPA. The name and address of the Office that administers FERPA are:

**Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, DC 20202-4605**

FERPA permits the District to disclose appropriately designated "directory information" without written consent, unless parents or eligible students have advised the School to the contrary in accordance with the District procedures outlined below. The primary purpose of directory information is to allow the District to include this type of information from your child's education records in certain school publications. Examples include:

- A playbill, showing your student's role in a drama production;
- The annual yearbook;
- Honor roll or other recognition lists;
- Graduation programs; and
- Sports activity sheets, such as for wrestling, showing weight and height of team members.

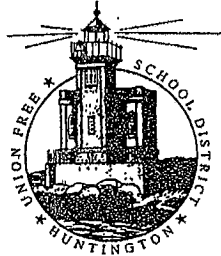
Directory information, which is information that is generally not considered harmful or an invasion of privacy if released, can also be disclosed to outside organizations without a parent's or eligible student's prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks.

In addition, pursuant to the federal *No Child Left Behind Act of 2001*, school districts receiving assistance under the federal *Elementary and Secondary Education Act of 1965* must provide military recruiters, upon request, with three directory information categories: names of secondary school students; 2) addresses of secondary school students; and 3) telephone listings of secondary school students. The District must release this information to military recruiters unless parents or students have advised the District they do not want the student's information disclosed without prior written consent.

If you do not want the District to disclose any or all directory information from your child's education records without your prior written consent, you must notify your child's building principal by September 30th.

The District has designated the following student information as directory information:

- name, address and telephone number
- date and place of birth
- major course of study
- participation in school activities or sports
- weight and height if a member of an athletic team
- dates of attendance
- degrees and awards received
- most recent school attended
- photograph (still or moving)
- class roster



Flower Hill Primary School

"A Tradition of Excellence Since 1657"

Mr. Marlon C. Small
Principal

Septiembre del 2013

Estimados padres/guardianes:

Atado usted va a encontrar una copia de la Notificación de los Derechos Según la Ley de Privacidad y Derechos Educativos familiares (FERPA por sus siglas en inglés) y La Ley de Ningún Niño Quedado Atrás del 2001(No Child Left Behind Act). FERPA permite a ambos padres y estudiantes mayores de dieciocho años ciertos derechos con respecto a los registros educativos del estudiante. Uno de ellos es el derecho de consentimiento para revelar identificable información personal contenida en los archivos escolares del estudiante.

FERPA también autoriza al distrito a revelar "información de directorio" designada apropiadamente sin necesidad de un consentimiento por escrito, a menos que los padres o el estudiante elegible han aconsejado a la escuela para no hacerlo. Si usted no desea que distrito revele cualquier o toda la información de directorio de los registros educativos de su hijo sin su consentimiento previo, deba notificar por escrito al distrito. Por favor envíe una carta a la escuela de Flower Hill antes del viernes, 27 de septiembre de 2013.

Si usted tiene alguna pregunta o inquietud con respecto a este tema, Por favor llame a la escuela al 673-2050. Gracias, por adelanto, por su cooperación anticipada.

Sinceramente

Marlon C. Small

Principal

Distrito Escolar de Huntington

"Una Tradición por Excepcencia Desde 1657"

Notificación de los Derechos Según la Ley de Privacidad y Derechos Educativos y la Ley de Ningún Niño Se Queda Atrás de 2001

La ley de Privacidad y Derechos Educativos (FERPA por sus siglas en inglés) otorga a los padres y estudiantes mayores de 18 años o estudiantes inscritos en una institución de educación post-secundaria (estudiantes elegibles) ciertos derechos con respecto a los archivos escolares del estudiante. Estos derechos incluyen:

1. Derecho a revisar y examinar los archivos escolares del alumno(a) en un lapso de 45 días a partir del día en que la escuela recibe el pedido para revisar dichos documentos. Los padres o estudiantes elegibles deben de presentar una solicitud por escrito al director(a) de la escuela especificando el archivo que desean revisar. El Director(a) de la Escuela hará las acomodaciones necesarias e informará a los padres o estudiante elegible a qué hora y dónde pueden revisar los archivos.
2. Derecho a solicitar la corrección de los archivos escolares del estudiante que los padres o estudiante elegible consideren inexactos o engañosos. Los padres o estudiantes elegibles pueden pedirle a la Escuela que corrija un archivo si creen que el mismo es inexacto o engañoso. Deben de presentar una solicitud escrita al Director de la Escuela especificando la parte del archivo que desean que se cambie y también especificar la razón por la que el mismo es inexacto o engañoso. Si la Escuela decide no corregir el archivo según lo solicitado por el padre o estudiante elegible, la Escuela les avisará de la decisión y les notificará de su derecho a tener una audiencia referente a la solicitud de enmienda. Los padres o estudiante elegible recibirán mayor información concerniente a los procedimientos de la audiencia cuando sean notificados de su derecho a tener una audiencia.
3. El derecho a dar permiso para revelar identificable información personal contenida en los archivos escolares del estudiante hasta donde FERPA lo permita sin tener un permiso. Un ejemplo de esto sería revelar información a autoridades escolares con intereses educativos legítimos. Una autoridad escolar es una persona empleada por la Escuela en calidad de administrador, supervisor, instructor o personal de apoyo (incluyendo el personal de salud o médico y personal de seguridad); una persona miembro de la Junta Directiva Educativa, una persona o compañía contratada por la escuela para prestar un servicio especial (como un abogado, auditor, médico o terapeuta); o un padre o estudiante miembro de un comité oficial, por ejemplo el comité de disciplina, o quejas, o alguna persona que coopere con otra autoridad escolar para que la misma cumpla con su deber. Una autoridad escolar tiene un interés educativo legítimo si la autoridad necesita revisar un archivo escolar con el fin de cumplir con sus responsabilidades profesionales. Sobre la solicitud, la escuela puede revelar los archivos escolares sin consentimiento a la autoridades de otro distrito escolar donde el estudiante busce o intenta de matricularse o se ha matriculado, si la revelación es por propósito de la matriculación del estudiante o traslado.
4. El derecho de presentar una queja ante el Departamento Federal de Educación si se considera que la Escuela no cumple con los requisitos de la FERPA. El nombre y dirección de la Oficina que administra la FERPA es:

**Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, DE 20202-4605**

FERPA autoriza al Distrito a revelar "información de directorio" designada apropiadamente sin necesidad de un consentimiento, a menos que los padres o estudiantes elegibles hayan solicitado lo contrario de acuerdo con los procedimientos del Distrito descritos a continuación. El fin básico de la información de directorio es permitir que el distrito incluya este tipo de información de los archivos de su hijo(a) en ciertas publicaciones escolares. Por ejemplo:

- Una obra de teatro que muestre el papel del estudiante en una producción dramática,
- El Libro Escolar Anual,
- Listas de Honores o de reconocimiento,
- Programas de Graduación y
- Hojas de actividades deportivas, como lucha libre, donde se muestra el peso y tamaño de los miembros del equipo.

Asimismo, la información de directorio, que es información que por lo general no se considera que pueda herir o invadir la privacidad si se revela, puede ser revelada a organizaciones externas sin previo consentimiento escrito de los padres o estudiantes elegibles. Organizaciones externas incluyen, pero no se limitan a compañías que fabrican los anillos de la clase o las que publican los libros escolares anuales.

Además, en cumplimiento con *la Ley de Ningún Niño se Queda Atrás de 2001*, los distritos escolares que reciban ayuda de parte de *la Ley Federal de Educación Elementaria y Secundaria de 1965* deben de proporcionar información del directorio a los oficiales de reclutamiento militar, si éstos solicitan, en tres categorías: 1) nombres de estudiantes de la secundaria, 2) direcciones de los estudiantes de secundaria, 3) números telefónicos de los estudiantes de la secundaria. El Distrito debe de revelar esta información a los oficiales de reclutamiento militar a menos que los padres hayan solicitado lo contrario previamente y por escrito.

Si no desea que el Distrito revele parte o nada de la información del directorio de los archivos de su hijo(a) sin su consentimiento, usted DEBE notificar al Distrito POR ESCRITO, EN UNA CARTA DIRIGIDA AL DIRECTOR DE LA ESCUELA DEL ESTUDIANTE ANTES DEL 30 DE SEPTIEMBRE.

El Distrito ha designado la siguiente información de los estudiantes como información del directorio:

- nombre, dirección y número de teléfono
- fecha y lugar de nacimiento
- curso principal de estudio
- participación en actividades escolares o deportes
- peso y tamaño si es miembro de un equipo atlético
- fechas de asistencia
- notas y premios recibidos
- última escuela a la que asistió
- fotografía (tipo)
- horario de clase.

**HUNTINGTON UNION FREE SCHOOL DISTRICT
AUTHORIZATION FOR RELEASE OF RECORDS**

I, _____, hereby authorize

the _____ to release copies
(name of school)

of _____
(list records)

which are part of the records of _____

and to furnish them to _____

for the purpose of _____

Signature

Date

This form must be signed by the parent/guardian or eligible student prior to the release of personally identifiable student information to a third party at the request of the parent/guardian or eligible student.)